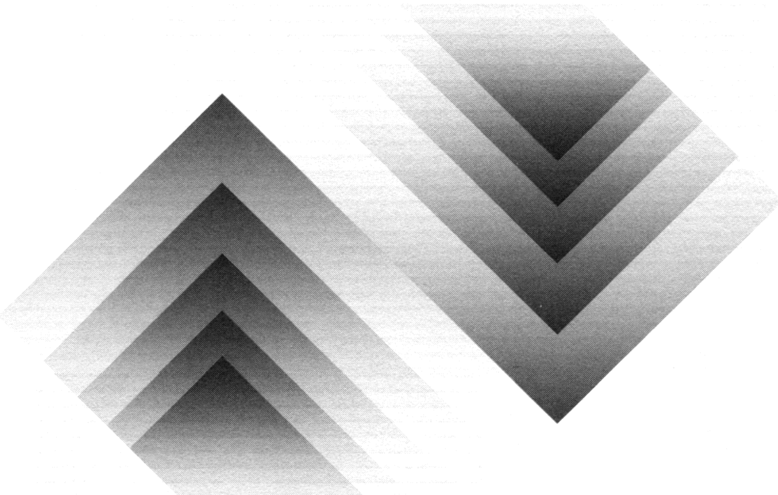
量子情報への
表現論的アプローチ

林　正人 著



共立出版

まえがき

群論的対称性は量子力学における基本的な概念であり，物理学の様々な分野で活用されてきた．量子系の特徴を積極的に用いて情報処理を行う量子情報においても，群論的対称性が重要な位置を占めることは間違いない．しかし，従来の量子情報の研究では，情報科学からの手法の導入や新規プロトコルの提案に重点が置かれ，群論的な対称性に十分には重きが置かれなかった．量子情報の数学的な基礎付けについては，主に作用素代数の観点からなされてきた．もちろん，量子情報の個別の研究においては，群論的手法の導入は進んでいる．しかし，体系的に量子情報における群論的手法をまとめた書籍は英文のものも含めて存在しない．また，いくつかの量子情報のテーマではその根幹の部分で群論的な考え方が基礎となっているにも関わらず十分に意識されていないことが多い．このようなテーマでは，群論的構造を意識することで，より深くその問題が理解できるだけでなく，一般化が容易に可能となる．従来，群論的構造を意識しなかったために，本質的なところで共通の基盤を持つテーマであるにも関わらず，まったく別のテーマとして取り扱われていた内容も少なくない．そのような事情を鑑みて本書では，群論的考え方が量子情報の基本的なインフラとして機能するように，量子情報の様々な概念を群論的対称性の観点から統一的に捉え直すことを試みた．

本書では，最初に第１章で，測定，状態，合成系，計算基底，エンタングルメントなどの量子情報の基礎概念を説明し，量子系を記述するための数学的な

記号を準備する．そして，第 2 章で量子情報の基礎となる量子通信路や情報量に関する基礎的内容をまとめる．ここまでは，線形代数や微積分，確率統計の初歩的な知識だけで理解できる．これらの準備の後，以下の章では，表現論の知識を仮定して，個別の量子情報のテーマについて扱う．しかし，表現論の知識を有しない読者はここで不安に思う必要はない．本書で必要となる表現論の知識は姉妹編『量子論のための表現論』で基礎から始めて全てまとめられている．この書籍と合わせて読めば，表現論の知識を一切仮定せず，本書の内容は全て，線形代数や微積分，確率統計の初歩的な知識だけで理解できる．なお，本書では表現論に関する文献参照は初出が他の文献である場合であっても，簡便のため全て上記の書籍に統一した．

実は，第 3 章以後の個々の章の内容を表現論なしで記述するには，かなりのページ数を要する．だが，表現論を経由することで，内容がコンパクトにまとめられ，それぞれの章の内容を 1 つの章に収めることが可能となった．このような構成からも，量子情報において表現論的な考え方が極めて重要な役割を果たすことがわかる．このように群の表現論を軸に量子情報を展開した点で，本書は類書にない特色がある．一方，量子情報のテーマは他の物理のテーマに比べ，数学的に厳密な取り扱いがなされることが多く，数学的にも興味深い対象となり得る．しかし，量子情報は数学者の興味，関心を得ていないのが現状である．その主な理由は，従来の研究では各論が先行し，それらの背後にある数学的構造が書かれた書籍がない点にある．本書では，表現を通じて量子情報の数学的構造を明らかになるような構成とした．

以下，量子情報の個別のテーマを扱う第 3 章以後の章の構成について述べる．第 3 章では，表現論を用いることで量子系のエンタングルメントを扱う．従来の量子情報のテキストでは主に，2 体間のエンタングルメントのみを扱ったものが主流であったが，多体系のエンタングルメントについても，表現論を用いて扱う．第 4 章では，群の表現について共変的な測定を定義し，最適測定の理論を与える．そして，群上の Fourier 変換と群作用の推定の関係について詳しく述べる．また，近似的な状態複製についても述べる．第 5 章では，量子誤り訂正について述べる．最初に古典系での代数的な誤り訂正について述べ，その後に，離散 Heisenberg 表現に基づいて，量子誤り訂正符号の典型例である Stabilizer 符号およびその特殊例である CSS 符号について述べる．さらに，代数的な量子誤り訂正の一般的な枠組みである，Clifford 符号についても述べ

る．その後に，CSS 符号の知識に基づいて量子暗号の安全性評価を扱う．第 6 章では，Schur 双対に基づくユニバーサル情報処理について扱う．ここで述べる内容は，主に，Csiszár と Körner によるタイプ理論の量子版と見なせる内容である．具体的には，密度行列の固有値の推定，量子状態の仮説検定，エンタングルメント集中化，量子系での情報源符号化，古典-量子通信路符号化が挙げられる．

なお，特に込み入ったテーマを扱った部分については，節や例のタイトルに*を付すことにした．この部分は，後の部分でも，*を付した部分にのみ使われる内容であるので，*を付した部分を飛ばして読んでも理解できるように構成されている．初学者にはなるべく，*を付した部分を飛ばして読むことを勧める．

このように，本書では表現論に基づいて，いくつかの量子情報のテーマについて扱った．本書を通じて，一人でも多くの方が量子情報に興味を持って頂けたら著者の望外の喜びである．最後に，本書をまとめるにあたってご協力して頂いた多くの方々に感謝の意を表したい．とりわけ，東京工業大学の松本隆太郎准教授，徳島大学の渡辺峻博士には，本書をまとめる上で適切な助言を頂いた．また，共立出版(株)の寿日出男氏，赤城圭氏には原稿をまとめる上で大変お世話になった．これらの方々には感謝の意を表したい．

林　正人

目　次

第1章

量子系の数学的基礎

1.1 系，状態および測定

量子情報の本題に入る前に，準備として，量子系の数学的基礎について簡単に要約したい．内容的に，拙著『量子論のための表現論』[37] の第1章と重複する部分が多いので，その本の第1章を既に読まれた読者は，本章の大半を飛ばして読み進めることができる．しかし，一部に [37] の第1章には記載されていない内容があるので，その部分についてはきちんと読んでもらいたい．本章の内容についてより詳しく学びたい方は，和書では石坂他『量子情報科学入門』[70] の第4章を読まれることをお勧めする．

さて，ミクロな物理系を記述する量子論では，記述する対称を**量子系**または，**系**とよび，それは数学的にはエルミート内積が定義された複素ベクトル空間 $\mathcal{H}$ で与えられる．$\mathcal{H}$ は有限次元の場合もあるが無限次元の場合もあり，有限次元の場合も含めそのような複素ベクトル空間 $\mathcal{H}$ は **Hilbert 空間**とよばれる[1)]．$\mathcal{H}$ はエルミート内積付きベクトル空間であるから，正規直交基底系 $\{e_i\}$ がとれる．それぞれの正規化された基底 e_i は互いに識別可能な量子系の状態を表す．一般の系の状態は，正規化されたベクトル $x \in \mathcal{H}$ で与えられる．基準となる正規直交基底系（基準基底系）を1つ定めると，一般の状態を表すベクトル x はそれらの重ね合わせ（線形結合）$\sum_i x_i e_i$ で表される．量子論では，

---

1) 無限次元の場合は与えられたエルミート内積の下での**完備性**も満たすとする．

$\mathcal{H}$ の要素 x に対して，2通りの表し方を用いる．1つはケットベクトル $|x\rangle$ による表記であり，もう1つはブラベクトル $\langle x|$ による表記である．これらの表記は実数係数に関する線形性を保つように定義されるが，複素数倍については $a \in \mathbb{C}$ について，

$$|ax\rangle = a|x\rangle, \quad \langle ax| = \bar{a}\langle x| \tag{1.1}$$

を満たすように定義する．特に，基準基底 e_i に対しては $|e_i\rangle, \langle e_i|$ とせず，$|i\rangle$, $\langle i|$ と記すことにする．

一方，$x, y \in \mathcal{H}$ のエルミート内積 $\langle x|y\rangle$ を $a, b \in \mathbb{C}$ について，$\langle ax|by\rangle = \bar{a}b\langle x|y\rangle$ となるように定義すると，x と y の内積 $\langle x|y\rangle$ はブラベクトルとケットベクトルを掛け合わせたもの $\langle x|\cdot|y\rangle$ と見なすことができる．

そして，量子系 $\mathcal{H}$ の状態，すなわち，系の様子は，$\mathcal{H}$ 上のトレースが 1 で対角成分が全て 0 以上となるエルミート行列 ρ で表される．対角成分が全て 0 以上となるエルミート行列を半正定値行列とよび，このようなエルミート行列 ρ は**密度行列**とよばれる．特に，密度行列 ρ のランクが 1 のとき，ρ は1次元射影となる．このような密度行列は**純粋状態**とよばれ，純粋状態以外の密度行列は**混合状態**とよばれる．純粋状態 ρ については，ρ の値域を表す正規化された $\mathcal{H}$ の要素 $|\phi\rangle$ と ρ を同一視することがあり，しばしば，正規化された $\mathcal{H}$ の要素 $|\phi\rangle$ を状態とよぶことがある．

一方，測定は $\mathcal{H}$ 上の半正定値行列 $\{M_\omega\}_{\omega\in\Omega}$ による単位行列 I の分解（すなわち，$\sum_{\omega\in\Omega} M_\omega = I$ を満たす）で与えられる [64]．このとき，Ω が測定値全体を表す集合であり，系の状態が ρ であるとき，測定値が ω となる確率は $\mathrm{Tr}\,\rho M_\omega$ で与えられる．ρ と M_ω がともに半正定値行列であることから，$\mathrm{Tr}\,\rho M_\omega$ は常に 0 以上の値となる．さらに，$\sum_{\omega\in\Omega} \mathrm{Tr}\,\rho M_\omega = \mathrm{Tr}\,\rho \sum_{\omega\in\Omega} M_\omega = \mathrm{Tr}\,\rho I = 1$ となり，これが確率の公理を満たすことが確認できる．このような半正定値行列による単位行列 I の分解 $\{M_\omega\}_{\omega\in\Omega}$ は**正作用素値測度 (Positive operator-valued measure: POVM)** とよばれる．特に，M_ω が全て射影である場合，**射影測定**または**射影値測度 (Projecton valued measure)** とよばれる．

次に，測定値の集合が一般の位相空間 Ω である場合について考えよう．この場合，離散的に測定値に対応する行列 M_ω を与えることはできない．Ω 上に積分 $\nu(d\omega)$ が与えられていれば，

$$\int_\Omega M_\omega \nu(d\omega) = I \tag{1.2}$$

を満たす $\{M_\omega\}$ は POVM となる．しかし，位相空間 Ω に値を持つ任意の POVM は必ずしも上の形で与えられるとは限らない．一般の POVM を与えるには測度論的扱いが必要となる．Ω は位相空間であるので，Ω の開集合から生成される Borel 集合族 $\mathcal{B}(\Omega)$ を考える．そして，$\mathcal{B}(\Omega)$ から $\mathcal{B}_+(\mathcal{H})$ への写像 M で以下を満たすものを POVM とよぶ．

(M1) $B_j \in \mathcal{B}(\Omega)$ が異なる j, l について $B_j \cap B_l = \emptyset$ のとき，$\sum_j M(B_j) = M(\bigcup_j B_j)$.

(M2) $M(\emptyset) = 0$.

(M3) $M(\Omega) = I$.

特に，任意の $B \in \mathcal{B}(\Omega)$ に対して，$M(B)$ が射影であるとき，M は PVM となる．一般の POVM M に対して，Hilbert 空間を適切に拡大することで，M は拡大された空間上の PVM E の制限として記述することができる [90].

この PVM の定義を用いて，$\mathcal{H}$ が無限次元の場合の作用素の対角化であるスペクトル分解を与えることができる．$\mathcal{H}$ 上の自己共役作用素 A は一般には固有ベクトルを持つとは限らない．しかし，$\mathcal{H}$ 上の自己共役作用素 A に対して，$\mathbb{R}$ に値を持つ PVM E が一意に存在し，以下を満たす．

$$A = \int_{\mathbb{R}} x E(dx). \tag{1.3}$$

なお，この事実は有界でない自己共役作用素についても成り立つ [59]．また，A がユニタリ作用素の場合は，$\mathbb{R}$ を単位円周 $U = \{z \in \mathbb{C} \mid |z| = 1\}$ に置き換えると同じ事実が成り立つ．このようにして，無限次元の場合の自己共役作用素として与えられる物理量の測定が与えられる．この場合も，状態が密度行列 ρ で与えられている場合，期待値，分散は $\mathrm{Tr}\, A\rho$, $\Delta_\rho^2 A := \mathrm{Tr}(A - (\mathrm{Tr}\, A\rho)I)^2\rho$ で与えられる．

実は，POVM は単に測定値が従う確率分布を与えるだけではなく，数学的には，密度行列 ρ の凸分解を与えることが可能である．すなわち，$\sum_\omega M_\omega = I$ であることから，

$$\operatorname{Tr} M_\omega \rho \sum_\omega \frac{\sqrt{\rho} M_\omega \sqrt{\rho}}{\operatorname{Tr} M_\omega \rho} = \sum_\omega \sqrt{\rho} M_\omega \sqrt{\rho} = \sqrt{\rho} I \sqrt{\rho} = \rho. \tag{1.4}$$

事実，任意の ρ の凸分解 $\rho = \sum_\omega p_\omega \rho_\omega$ に対して，$M_\omega := \rho^{-\frac{1}{2}} p_\omega \rho_\omega \rho^{-\frac{1}{2}}$ と与えると，(1.4) を用いて，凸分解 $\rho = \sum_\omega p_\omega \rho_\omega$ を再構成することができる．

1.2　合成系

2つの互いに識別可能な量子系 $\mathcal{H}_A$ と $\mathcal{H}_B$ を考えよう．例えば，系 $\mathcal{H}_A$ がある粒子の内部自由度を表していて，系 $\mathcal{H}_B$ がその粒子の位置に関する自由度を表しているとすると，その粒子全体の自由度を表す量子系が必要となる．そのような量子系は系 $\mathcal{H}_A$ と $\mathcal{H}_B$ の合成系とよばれる．合成系はテンソル積空間 $\mathcal{H}_A \otimes \mathcal{H}_B$ で与えられる．テンソル積空間 $\mathcal{H}_A \otimes \mathcal{H}_B$ とは $\mathcal{H}_A$ と $\mathcal{H}_B$ のそれぞれの正規直交基底を $\{|v_i\rangle\}_{i=1}^k$ と $\{|u_j\rangle\}_{j=1}^l$ とすると，$\{|v_i, u_j\rangle\}_{1\le i\le k, 1\le j\le l}$ が正規直交基底となる空間である．

次に系 $\mathcal{H}_A$ と系 $\mathcal{H}_B$ に独立に状態 ρ と σ が準備された場合を考えよう．この場合，$\rho = \sum_{i,i'=1}^k a_{i,i'} |v_i\rangle\langle v_{i'}|$, $\sigma = \sum_{j,j'=1}^l b_{j,j'} |u_j\rangle\langle u_{j'}|$ であるとすると，合成系上の状態は**テンソル積状態** $\rho\otimes\sigma := \sum_{i,i'=1}^k \sum_{j,j'=1}^l a_{i,i'} b_{j,j'} |v_i, u_j\rangle\langle v_{i'}, u_{j'}|$ で与えられる．なお，合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の状態はテンソル積状態 $\rho\otimes\sigma$ やその凸結合 $\sum_j p_j \rho_j \otimes \sigma_j$ で記述できる状態（**セパラブル状態**）だけではない．（p_j は確率を表し，ρ_j, σ_j はそれぞれ，$\mathcal{H}_A, \mathcal{H}_B$ 上の密度行列を表す．）例えば，ベクトル $\sum_j \sqrt{p_j} |v_j, u_j\rangle$ で与えられる純粋状態はテンソル積状態の凸結合として表せないので，セパラブル状態ではない．そのような状態は**エンタングル**した状態といわれ，量子情報処理の資源として，大変盛んに研究されている．特に，状態のそのような性質を**エンタングルメント**とよぶ．

合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の状態が密度行列

$$\rho = \sum_{i,i'=1}^k \sum_{j,j'=1}^l c_{i,j,i',j'} |v_i, u_j\rangle\langle v_{i'}, u_{j'}|$$

で与えられているとき，任意の系 $\mathcal{H}_A$ 上の行列 X に対して，

$$\operatorname{Tr}(\operatorname{Tr}_{\mathcal{H}_B} \rho) X = \operatorname{Tr} \rho (X \otimes I_{\mathcal{H}_B})$$

を満たす系 $\mathcal{H}_A$ 上の状態は，以下を満たす状態 $\mathrm{Tr}_{\mathcal{H}_B}\,\rho$ が存在する．この場合，系 $\mathcal{H}_A$ だけに注目したときは，系 $\mathcal{H}_A$ 上の状態は $\mathrm{Tr}_{\mathcal{H}_B}\,\rho$ で与えられると考えるのが妥当である．状態 $\mathrm{Tr}_{\mathcal{H}_B}\,\rho$ は ρ の**部分トレース**とよばれ，以下の方法で具体的に計算できる．

$$\mathrm{Tr}_{\mathcal{H}_B}\,\rho = \sum_{i,i'=1}^{k}\sum_{j=1}^{l} c_{i,j,i',j}|v_i\rangle\langle v_{i'}|.$$

なお，ρ が基底 $\{|v_i, u_j\rangle\}_{i,j}$ の下で対角である場合は，部分トレースは対角成分からなる確率分布の周辺分布と一致する．部分トレースをとって得られる密度行列を**縮約密度行列**とよぶ．以下，混乱の恐れがないときは，$\mathcal{H}_B$ を下付き添え字として用いる場合，B と省略する．

本書では，混乱が生じない限り，$\mathcal{H}_A$ 上の行列 X と，$\mathcal{H}_B$ 上の行列 Y に対して，$\mathcal{H}_A \otimes \mathcal{H}_B$ 上の行列 $X \otimes I_{\mathcal{H}_B}$, $I_{\mathcal{H}_A} \otimes Y$ を単純に X, Y と略記する．そのため，$X \otimes Y$ は XY と書く．

以下，$\mathcal{H}_A, \mathcal{H}_B$ の基準基底が与えられた場合に，用いられる省略記号について述べる．この場合，2 つの量子系を扱うので，それぞれの基準基底を表すケットベクトルを $|j\rangle_A, |j\rangle_B$ と記し，注目している系を区別する．そのため合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ の基底は $|k\rangle_A \otimes |j\rangle_B$ で与えられるが，簡単のため $|k, j\rangle_{A,B}$ と記すことにする．

以下の議論では，行列 $X = (x_{k,j})$ について，$\overline{X}$ は基準基底についての X の行列成分の**複素共役**をとって得られる行列を表し，X^T は基準基底についての X の**転置行列**を表す．そして，$X^\dagger$ は X の**共役転置行列**を表す．$\overline{X}$ と X^T は基準基底のとり方に依存するが，$X^\dagger$ はエルミート内積のとり方にのみ依存する．そして，合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上のベクトル $\sum_{k,j} x_{k,j}|k, j\rangle_{A,B}$ を $|X\rangle\rangle_{A,B}$ と記すことにする．

$$Y \otimes Z|X\rangle\rangle_{A,B} = |YXZ^T\rangle\rangle_{A,B} \tag{1.5}$$

が成り立つ．2 つのベクトル $|X\rangle\rangle_{A,B}$, $|Y\rangle\rangle_{A,B}$ の内積は ${}_{A,B}\langle\langle X|Y\rangle\rangle_{A,B} = \mathrm{Tr}\,X^\dagger Y$ となる．

したがって，ベクトル $|X\rangle\rangle_{A,B}$ が状態ベクトルになる（すなわち，ノルムが 1 となる）条件は $\mathrm{Tr}\,X^\dagger X = 1$ となることである．部分トレースについては以下の公式が成り立つ．

$$\mathrm{Tr}_B |X\rangle\rangle_{A,B\ A,B}\langle\langle X| = XX^\dagger, \quad \mathrm{Tr}_A |X\rangle\rangle_{A,B\ A,B}\langle\langle X| = X^T\overline{X}. \qquad (1.6)$$

ここで，$XX^\dagger$ および $X^\dagger X$ を等長行列 U, V を用いて固有値が大きい順に対角化しよう．

$$U^\dagger XVV^\dagger X^\dagger U = U^\dagger XX^\dagger U = D, \quad = V^\dagger X^\dagger UU^\dagger XV = D.$$

ここで，D は対角成分を大きい順に並べた対角行列であり，その対角成分は全て非負である．D の次元は $\mathcal{H}_A$, $\mathcal{H}_B$ の次元よりも同じか小さい．行列 D のランクを状態ベクトル $|X\rangle\rangle$ の **Schmidt ランク**とよぶ．Schmidt ランクは $\mathcal{H}_A$ と $\mathcal{H}_B$ の双方の次元よりも小さい．D の対角成分をその **Schmidt 係数**とよぶ．$U^\dagger XV$ とその共役転置行列 $V^\dagger X^\dagger U$ は可換となるので，$U^\dagger XV$ の対角成分の絶対値の二乗は D の固有値に一致する．ここで，絶対値が 1 となる対角行列 D' を考えることにより，$X = UD'\sqrt{D}V^\dagger$ を得る．等長行列 UD' を新たに U と置き直すことにより，X の **Schmidt 分解**

$$X = U\sqrt{D}V^\dagger \qquad (1.7)$$

を得る．この事実を一般の $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の純粋状態 $|a\rangle$ に適用しよう．$|a\rangle$ に対して，以下を満たす $\mathcal{H}_A$, $\mathcal{H}_B$ の正規直交基底 $\{|v_i\rangle\}$, $\{|u_j\rangle\}$ と Schmidt 係数 $d_1, \ldots, d_k$ が存在する．$\mathcal{H}_A$ の次元 k が $\mathcal{H}_B$ の次元 l より小さいとすると，

$$|a\rangle = \sum_{j=1}^{k} d_j |v_j\rangle \otimes |u_j\rangle. \qquad (1.8)$$

量子情報の文献では (1.7) よりもむしろ (1.8) を Schmidt 分解とよぶことが多い．(1.8) における $\{|v_i\rangle\}$, $\{|u_j\rangle\}$ を **Schmidt 基底**とよぶ．

$\mathcal{H}_A$ 上の混合状態 ρ に対して，テンソル積空間 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の純粋状態 $|X\rangle\rangle_{A,B}$ が

$$\rho = \mathrm{Tr}_B |X\rangle\rangle_{A,B\ A,B}\langle\langle X| \qquad (1.9)$$

を満たすとき，純粋状態 $|X\rangle\rangle_{A,B}$ を $\mathcal{H}_B$ の**参照系**とする ρ の**純粋状態化**とよぶ．上記の議論より，純粋状態 $|X\rangle\rangle_{A,B}$ が ρ の純粋状態化となるための必要十分条件は $XX^\dagger = \rho$ となることである．この条件は $X^\dagger X$ の値域をサポートとする部分等長写像 V を用いて，X が以下のように書けることと同値である．

$$X = \sqrt{\rho}V. \qquad (1.10)$$

この事実は，ρ の純粋状態化は部分等長写像による作用で移りあう自由度を除いて一意に決まることを示している．

特に，$\mathcal{H}_A$ と $\mathcal{H}_B$ の双方の次元が d であり，(1.7) を満たす D の対角成分が全て $\frac{1}{d}$ であるとき，$|X\rangle\rangle_{A,B}$ は**最大エンタングル状態**という．この条件は，X がユニタリ行列となることと同値である．

1.3 多体系

n 個の粒子があり，個々の粒子の状態を表す量子系 $\mathcal{H}_i$ $(i = 1, \ldots, n)$ が与えられた場合を考える．これらの粒子が互いに識別可能である場合，n 個の粒子からなる合成系は $(((\mathcal{H}_1 \otimes \mathcal{H}_2) \cdots) \otimes \mathcal{H}_n)$ で与えられる．このとき，テンソル積空間はテンソル積のとる順番に依存しないため，上記の空間は $(\mathcal{H}_1 \otimes (\cdots (\mathcal{H}_{n-1} \otimes \mathcal{H}_n)))$ と一致する．したがって，$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ と記す．特に，各 $\mathcal{H}_i$ が $\mathcal{H}$ と同型のときは，テンソル積空間は $\mathcal{H}^{\otimes n}$ と略すことにする．

各 $\mathcal{H}_i$ に状態 ρ_i が独立に準備されたときの合成系の状態は $(((\rho_1 \otimes \rho_2) \cdots) \otimes \rho_n)$ で与えられる．行列のテンソル積もテンソル積のとる順番に依存しないため，この密度行列を $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ と記す．特に $\rho_i = \rho$ であるとき，すなわち，同一状態 ρ が独立に n 個準備されたときの密度行列を $\rho^{\otimes n}$ と記す．この密度行列は状態 ρ の n 階**テンソル積状態**とよばれる．上記の記法は ρ や ρ_i が密度行列とならない一般の行列の場合についても用いることとする．

また，テンソル積空間 $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ 上の行列 A について特定の系 $\mathcal{H}_i$ についてのみの部分トレースを $\mathrm{Tr}_{\mathcal{H}_i} A$ と記す．逆に，特定の系 $\mathcal{H}_i$ 以外の全ての系についての部分トレースを $\mathrm{Tr}_{\check{\mathcal{H}}_i} A$ と記す．特に，A が密度行列 ρ である場合，$\mathrm{Tr}_{\check{\mathcal{H}}_i} \rho$ を $\rho_{\mathcal{H}_i}$ または ρ_i と記す．

一方，系 $\mathcal{H}_i$ 上の行列 A_i に対して，テンソル積空間 $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ 上の行列 $I^{\otimes i-1} \otimes A_i \otimes I^{\otimes n-i}$ を A_i と省略する．そして，$A_i = A$ であるとき，$\sum_{i=1}^n A_i$ を $A^{(n)}$ と記す．

1.4 文献の紹介

以下，簡単に表現論の視点から量子情報を扱った書籍を紹介する．量子情報

に関する書籍は数多くあるものの [91, 120, 121, 122, 70, 38, 36]，表現論の視点から扱ったものはさほど多くない．最初に本格的に表現論の視点から量子情報を扱った書籍は Holevo[64] であり，その第3章，第4章で有限次元系の表現論を用いて量子測定の最適化問題を扱っている．その後，いくつかの論文で量子情報の解析のために表現論が用いられた．その次に，基礎から丁寧に有限次元系の表現論による量子情報を扱った書籍としては，Christandl [18] が挙げられる．また，Bose 粒子系での量子情報を扱った書籍としては，同じく，[64] の第5章，第6章が挙げられる．その他，近年の進展については，Wang [112] が挙げられる．

第2章

量子通信路, 情報量とその数学的構造

2.1 量子系での通信路

全ての量子系での操作は，初期状態を入力状態，終状態を出力状態と考えると，通信路と見なすことができる．すなわち数学的には，量子系での操作と通信路は同じ対象を扱っていることになる．以下では，用語を統一するため，**量子通信路**という表記を用いる．特に，量子論の主要な目的は，物理系の状態の時間発展やある環境下での変化を正確に予言する（記述する）ことにある．以下では量子通信路を入出力状態の関係を与える写像として定義するが，この定義は上述の目的に関して数学的に完全に完成された枠組みを与えることとなる．

入力系が $\mathcal{H}$ であり，出力系が $\mathcal{K}$ である場合，量子通信路は $\mathcal{H}$ 上の密度行列の集合 $\mathcal{S}(\mathcal{H})$ から $\mathcal{K}$ 上の密度行列の集合 $\mathcal{S}(\mathcal{K})$ への写像 Λ で与えられる．この場合，凸結合 $\lambda\rho_1 + (1-\lambda)\rho_2$ $(0 < \lambda < 1)$ の意味を考えると，自然に等式 $\Lambda(\lambda\rho_1 + (1-\lambda)\rho_2) = \lambda\Lambda(\rho_1) + (1-\lambda)\Lambda(\rho_2)$ が成り立つ．

さらに，写像 Λ $\mathcal{H}$ 上のエルミート行列の空間 $\mathcal{B}(\mathcal{H})$ から，$\mathcal{K}$ 上のエルミート行列の空間 $\mathcal{B}(\mathcal{K})$ へ拡大すると，以下の

線形性： $\Lambda(aA + bB) = a\Lambda(A) + b\Lambda(B)$

が成り立つことが知られている．（ここで，a, b は任意の実数であり，A, B は

$\mathcal{B}(\mathcal{H})$ の要素である．）しかし，単純に線形性を満たす写像 Λ が量子通信路を与えるわけでない．

少なくとも，$\mathcal{S}(\mathcal{H})$ の要素は $\mathcal{S}(\mathcal{K})$ の要素に移らなければならない．この条件は，以下の2つの条件の組み合わせと同値である．

正値性：　$A \geq 0 \Rightarrow \Lambda(A) \geq 0.$

トレース保存性：　$\mathrm{Tr}\, A = \mathrm{Tr}\, \Lambda(A).$

しかし，この3つの条件を満たすだけでは，必ずしも量子通信路とはいい切れない．この部分が量子系の難しいところである．

ここで，補助系 $\mathbb{C}^n$ を考えよう．補助系との合成系 $\mathcal{H} \otimes \mathbb{C}^n$ での量子通信路を考える．補助系と系 $\mathcal{H}$ の間には相互作用がないとし，補助系では状態の変化が起こらないとする．そして，$\Lambda \otimes id_n(A \otimes B) := \Lambda(A) \otimes B$ とすると，合成系 $\mathcal{H} \otimes \mathbb{C}^n$ での量子通信路は $\Lambda \otimes id_n$ で与えられる．そのため，この写像 $\Lambda \otimes id_n$ も正値性を満たす必要がある．

n 正値性：　$X \geq 0 \Rightarrow \Lambda \otimes id_n(X) \geq 0.$ ただし，X は $\mathcal{H} \otimes \mathbb{C}^n$ 上の行列である．

特に，任意の n について n 正値性を満たす条件を完全正値性とよぶ．

完全正値性：　任意の n について n 正値性が成り立つ．

これらの議論から，量子通信路は線形性，完全正値性，トレース保存性を満たすことが確認できる．実は，その逆に，線形性，完全正値性，トレース保存性を満たす Λ に対応する量子通信路が原理的に存在することが知られている．そして，系 $\mathcal{H}$ から系 $\mathcal{H}_1$ への量子通信路の集合を $\mathcal{T}(\mathcal{H}, \mathcal{H}_1)$ と記す．

系 $\mathcal{H}$ から系 $\mathcal{K}$ への量子通信路 Λ が与えられたとき，系 $\mathcal{H}$ と同次元の参照系 $\mathcal{R}$ が与えられ，初期状態がその合成系 $\mathcal{H} \otimes \mathcal{R}$ 上の最大エンタングル状態の定数倍 $|I\rangle\rangle := \sum_l |l, l\rangle_{H,R}$ である場合の合成系 $\mathcal{K} \otimes \mathcal{R}$ 上の（正規化されていない）終状態 $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ に注目する．この状態は，後に述べるように Λ に関する情報を全て含んでいるため，Λ の **Choi-Jamiolkowski 表現**とよばれる [15, 71]．入力系の次元が有限の場合，この正規化されていない状態のトレースは入力系の次元に一致する．

$\mathcal{H}$ 上の入力状態が $|u\rangle_H = \sum_l u_l |l\rangle_H$ である場合の出力状態を記述するため

に，$|\overline{u}\rangle_R = \sum_l \overline{u}_l |l\rangle_R$ を用いた以下の公式を準備する．

$$|u\rangle_H \ {}_H\langle u| = {}_R\langle \overline{u}|(|I\rangle\rangle\langle\langle I|)|\overline{u}\rangle_R = \mathrm{Tr}_{\mathcal{R}}(|I\rangle\rangle\langle\langle I|)I \otimes |\overline{u}\rangle_R \ {}_R\langle \overline{u}|. \tag{2.1}$$

すると，$\mathrm{Tr}_{\mathcal{R}}$ と $(\Lambda \otimes id)$ の順序を入れ替えることで，Λ の出力状態は以下のように表せる．

$$\begin{aligned}\Lambda(|u\rangle_H \ {}_H\langle u|) &= \mathrm{Tr}_{\mathcal{R}}(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)I \otimes |\overline{u}\rangle_R \ {}_R\langle \overline{u}| \\ &= {}_R\langle \overline{u}|(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)|\overline{u}\rangle_R.\end{aligned}$$

Λ が完全正写像であることから，

$$(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|) \geq 0 \tag{2.2}$$

となり，Λ がトレースを保存性することから，

$$\mathrm{Tr}_{\mathcal{K}}(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|) = I \tag{2.3}$$

となる．したがって，(2.2), (2.3) を満たす $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ を用いることで，完全正写像 Λ を記述することができる．

次に，Λ の Choi-Jamiolkowski 表現 $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ の参照系を $\mathcal{E}$ とする純粋状態化を $|U\rangle\rangle_{(E,K),R}$ とする．U は $\mathcal{R}$ から $\mathcal{E} \otimes \mathcal{K}$ への線形写像と見なせる．特に，Choi-Jamiolkowski 表現の参照系を**環境系**とよぶ．すると，Λ は

$$\Lambda(\rho) = \mathrm{Tr}_E \, U\rho U^\dagger \tag{2.4}$$

で与えられる．Λ がトレースを保存する完全正写像であるとき，$\mathrm{Tr}\,\rho = \mathrm{Tr}\,U\rho U^\dagger$ であるので，U は等長写像である．以下では，環境系 $\mathcal{E}$ と系 $\mathcal{H}$ から $\mathcal{E} \otimes \mathcal{K}$ への等長写像 U で (2.4) を満たすものを Λ の **Stinespring 表現**とよぶ [108]．

そして，Λ の Stinespring 表現 $\mathcal{E}, U$ に対して，$\mathcal{E}$ の正規直交基底 $\{|m\rangle_E\}$ を用いると，Λ は以下のように書ける．

$$\Lambda(\rho) = \sum_{m,m'} {}_E\langle m'|U\rho U^\dagger|m\rangle_E. \tag{2.5}$$

$F_m := {}_E\langle m|U$ とすると，

$$\Lambda(\rho) = \sum_m F_m \rho F_m^\dagger \tag{2.6}$$

となる．さらにトレース保存性条件から，$\{F_m\}$ は条件

$$\sum_m F_m^\dagger F_m = I \tag{2.7}$$

を満たす．以下では，(2.7) の右辺を Λ の **Kraus 表現**という [80].

逆に，(2.7) を満たす $\{F_m\}$ を用いて Λ が (2.6) で与えられる場合，Λ はトレースを満たす完全正写像となる．

これらの議論をまとめると以下の定理を得る．（上記の各段落の議論は **(1)**⇒ **(2)**⇒ **(3)**⇒ **(4)**⇒ **(1)** の証明となっている．）

定理 2.1.1　エルミート行列からエルミート行列への線形写像 Λ について以下の3条件は同値である．

(1)　Λ は完全正写像である．

(2)　Λ の Choi-Jamiolkowski 表現 $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ が (2.2), (2.3) を満たす．

(3)　Λ に対して，(2.4) を満たす系 $\mathcal{E}$ と系 $\mathcal{H}$ から $\mathcal{E} \otimes \mathcal{K}$ への等長写像 U（Stinespring 表現）が存在する．

(4)　Λ が (2.7) を満たす $\{F_m\}$ を用いて (2.6) で与えられる．（Kraus 表現が存在する．）

上記の Stinespring 表現には物理的な意味がある．状態変化 Λ が起きるときには，最初に環境系との相互作用が起き $\mathcal{H}$ 上の入力状態 ρ が等長写像 U により，$\mathcal{E} \otimes \mathcal{K}$ に移る．そして，受信者は系 $\mathcal{K}$ のみ受信するので，環境系 $\mathcal{E}$ について部分トレースをとることになり，出力状態 $\Lambda(\rho)$ を受け取る．したがって，環境系に漏れた情報は以下のトレースを保存する完全正写像 Λ_E で与えられる．この通信路は盗聴があった場合での情報漏洩の評価にも用いられる．

$$\Lambda_E(\rho) := \mathrm{Tr}_{\mathcal{K}}\, U\rho U^\dagger.$$

Kraus 表現 $\{F_m\}$ を用いると $U = \sum_m F_m|m\rangle$ となることから，Λ_E は以下で与えられる．

$$\Lambda_E(\rho) = \sum_{m,m'} \mathrm{Tr}\, F_m \rho F_{m'}^\dagger |m\rangle\langle m'|. \tag{2.8}$$

このとき，Λ_E は以下に述べる意味で，Stinespring 表現のとり方に依存しない．そのため，Λ_E は (2.8) で与えられるとして一般性を失わない．2つ

の Stinespring 表現を考え，それぞれの環境系を $\mathcal{E}, \mathcal{E}'$ とし，入力状態が $\mathcal{R}$ と $\mathcal{H}$ との最大エンタングル状態であるときの全系でのそれぞれの終状態を $\rho_{R,E,K}$，$\rho'_{R,E,K}$ とする．これらはともに Λ の Choi-Jamiolkowski 表現 $\frac{1}{\dim \mathcal{H}}(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ の純粋状態化となる．純粋状態化の一意性より，環境系 $\mathcal{E}$ から環境系 $\mathcal{E}'$ への $V\rho_{R,E,K}V^\dagger = \rho'_{R,E,K}$ を満たす部分等長写像 V が存在する．それぞれの Stinespring 表現の下での環境系への写像を Λ_E, Λ'_E とすると，

$$V\Lambda_E(\rho)V^\dagger = \dim \mathcal{H} V \operatorname{Tr}_{K,R} \rho_{R,E,K}\overline{\rho}V^\dagger = \dim \mathcal{H} \operatorname{Tr}_{K,R} \rho'_{R,E,K}\overline{\rho} = \Lambda_E(\rho)'$$

となり，環境系が獲得する状態は互いに部分等長写像 V によって移りあう．

さらに，$\Lambda(\rho_{\mathrm{mix},H}) = \rho_{\mathrm{mix},K}$ となるとき，通信路 Λ は**ユニタル**という．

さらに，量子通信路 Λ が入力系 $\mathcal{H}$ 上の POVM $\{M_i\}$ と出力系 $\mathcal{K}$ 上の量子状態の集合 $\{\rho_i\}$ を用いて $\Lambda(\rho) = \sum_i (\operatorname{Tr} M_i\rho)\rho_i$ と書けるとき，**エンタングルメント破壊通信路**とよぶ．このとき以下の定理が成り立つ [38, Theorem 5.2].

定理 2.1.2　量子通信路 Λ がエンタングルメント破壊通信路であることと，量子通信路 Λ の Choi-Jamiolkowski 表現 $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ がセパラブルであることは同値である．

2.2　測定に伴う状態変化

量子系で POVM $\{M_\omega\}_{\omega\in\Omega}$ に対応する測定を行ったときの測定値 ω に応じた状態変化は，POVM からは一意には定まらない．その中でも最も典型的な状態変化は以下で与えられる．測定前の初期状態が ρ であるとき，測定値 ω を得た場合の終状態は

$$\frac{\sqrt{M_\omega}\rho\sqrt{M_\omega}}{\operatorname{Tr}\rho M_\omega} \tag{2.9}$$

で与えられる．上記を POVM $\{M_\omega\}_{\omega\in\Omega}$ に伴う**典型的な状態変化**とよぶことにする．特に，POVM が PVM $\{E_\omega\}_{\omega\in\Omega}$ で与えられる場合，(2.9) は

$$\frac{E_\omega\rho E_\omega}{\operatorname{Tr}\rho E_\omega} \tag{2.10}$$

と書け，**射影仮説**とよばれる．PVM で記述される測定は精密に測定器を構成すれば，これを満たす測定が可能と考えられている．この条件を満たす測定は**非破壊測定**とよばれる．このときの平均出力状態を与える写像 $\rho \mapsto \sum_\omega E_\omega \rho E_\omega$ は**ピンチング**とよばれる．特に，エルミート行列 X スペクトル分解 $\sum_i x_i E_i$ から定まる PVM $\{E_i\}$ によるピンチングを Λ_X と記すことにする．

しかし，測定器の性能が不十分である場合などは，(2.9) は成り立たない．一般の測定に伴う状態変化は，測定値 $\omega \in \Omega$ に応じて決まる完全正写像 Λ_ω の集合 $\{\Lambda_\omega\}_{\omega\in\Omega}$ を用いて以下のように表される．測定前の初期状態が ρ であるとき，測定値 ω を得た場合の終状態は

$$\frac{\Lambda_\omega(\rho)}{\operatorname{Tr}\Lambda_\omega(\rho)} \tag{2.11}$$

となり，測定値 ω が得られる確率は $\operatorname{Tr}\Lambda_\omega(\rho)$ で与えられる．この場合，$\sum_{\omega\in\Omega}\operatorname{Tr}\Lambda_\omega(\rho) = 1$ となることから，完全正写像 $\sum_{\omega\in\Omega}\operatorname{Tr}\Lambda_\omega$ がトレースを保存する必要がある．したがって，測定に伴う状態変化はトレースを保存する完全正写像の完全正写像による分解 $\{\Lambda_\omega\}_{\omega\in\Omega}$ を用いて (2.11) で与えられることになる．このような分解を **Instrument** とよぶことにする [96, 97, 98]．完全正写像は Kraus 表現を持つことから，適切に行列 $F_{m,\omega}$ を選ぶと，$\Lambda_\omega(\rho) = \sum_m F_{m,\omega}\rho F_{m,\omega}^\dagger$ となり，$\sum_{\omega,m} F_{m,\omega}^\dagger F_{m,\omega} = I$ が成り立つ．なお，Instrument は測定に伴う状態変化が起きた後に，ある量子通信路を施し得られる状態変化を加えたものも記述している．

2.3　凸集合と不等式

2.3.1　凸集合と凸関数

系 $\mathcal{H}$ 上の量子状態 ρ_1, ρ_2 と $1 \geq \lambda \geq 0$ に対して，**凸結合** $\lambda\rho_1 + (1-\lambda)\rho_2$ は量子状態となる．量子状態の集合のように，任意の2つの要素についての凸結合を含む集合を**凸集合**という．凸集合 X の点 x で $x = \lambda x_1 + (1-\lambda)x_2$ を満たす $x_1, x_2 \in X$ は x に限られるとき，x は X の**端点**という．X の端点の集合を $\operatorname{Ext}(X)$ と記す．例えば，系 $\mathcal{H}$ 上の量子状態の集合 $\mathcal{S}(\mathcal{H})$ の端点の集合 $\operatorname{Ext}(\mathcal{S}(\mathcal{H}))$ は純粋状態の集合となる．また凸集合 X が部分集合 S を用いて，$\{\sum_j p_j x_j \mid x_j \in S\}$ で与えられるとき，X を S の**凸包**という．

凸集合 X を含む実ベクトル空間の最小の次元が m のとき，m を X の次元とする．

そして，凸集合上で定義された実数値関数 f が任意の $1 > \lambda > 0$ を満たす λ について，$\lambda f(\rho_1) + (1-\lambda) f(\rho_2) \geq f(\lambda\rho_1 + (1-\lambda)\rho_2)$ を満たすとき，f を**凸関数**という．逆に，$-f$ が凸関数であるとき，f は**凹関数**であるという．例えば，非負の実数のなす集合 $\mathbb{R}_+ := \{x \in \mathbb{R} \,|\, x \geq 0\}$ 上で定義される関数 $x \mapsto x\log x$, $x \mapsto x^{1+s}$, $x \mapsto x^{-s}$ （ただし，$s > 0$ とする）は凸関数である．また，関数 $x \mapsto \log x$, $x \mapsto x^{1-s}$ （ただし，$1 > s > 0$ とする）は凹関数である．

演習問題 1　線形関数 f と凸関数 g の合成関数 $g \circ f$ は凸関数となることを示せ．

演習問題 2　行列 X について，関数 $\rho \mapsto |\operatorname{Tr} X\rho|^2$ は凸関数となることを示せ．

凸集合 X の端点集合 $\operatorname{Ext}(X)$ で定義された関数 f に対して，f の **convex roof** とよばれる凸集合 X 上の関数 $\operatorname{CR}(f)$ を以下で定義する．

$$\operatorname{CR}(f)(x) := \sup\left\{ \sum_j p_j f(x_j) \middle| \sum_j p_j x_j = x,\ x_j \in \operatorname{Ext}(X),\ p_j \geq 0 \right\}.$$

特に，X 上の関数 f が $f = \operatorname{CR}(f_{\operatorname{Ext}(X)})$ を満たすとき，**自己 convex roof** とよぶ．このとき以下の補題が定義から示せる．

補題 2.3.1　f の convex roof $\operatorname{CR}(f)$ は凸関数である．

さらに，以下の補題が成り立つ．

補題 2.3.2　凸集合 X の端点集合 $\operatorname{Ext}(X)$ で定義された関数 f と凸集合 X 上で定義された凸関数 g が任意の $x \in \operatorname{Ext}(X)$ について，$f(x) = g(x)$ を満たすとする．このとき，任意の $x \in X$ について，$\operatorname{CR}(f)(x) \geq g(x)$ が成り立つ．

証明.　$\operatorname{CR}(f)(x) = \sum_j p_j f(x_j)$ となる端点分解 $\sum_j p_j x_j = x$ に注目する．すると，g の凸性より，$g(x) \leq \sum_j p_j g(x_j) = \operatorname{CR}(f)(x)$ となり題意を得る．

□

次に，凸関数の概念を一般化するために，Majorization とよばれる概念を導入する．$\mathbb{R}_+^d$ に値を持つベクトル $\boldsymbol{a}=(a_j)$ が与えられたとき，$a_j^{\downarrow}$ を $a_1,\ldots,a_d$ の中で j 番目に大きい値を表すとしよう．そして，$\mathbb{R}^d$ に値を持つ2つのベクトル $\boldsymbol{a},\boldsymbol{b}$ に対し，任意の $k=1,\ldots,d$ について，$\sum_{j=1}^k a_j^{\downarrow} \ge \sum_{j=1}^k b_j^{\downarrow}$ および，$\sum_{j=1}^d a_j = \sum_{j=1}^d b_j$ が成り立つとき，$\boldsymbol{a}\succ\boldsymbol{b}$ と記す．このような関係を **Majorization** とよぶ．2つの密度行列 ρ_1, ρ_2 のそれぞれの固有値からなるベクトル $\boldsymbol{a},\boldsymbol{b}$ について，$\boldsymbol{a}\succ\boldsymbol{b}$ となるとき，$\rho_1\succ\rho_2$ と記す．

そして，$\mathbb{R}_+^d$ で定義される $\mathbb{R}$ に値を持つ関数 f で，置換 $g\in S_d$ について不変，すなわち，$f(g(\boldsymbol{a}))=f(\boldsymbol{a})$ となるものを**対称関数**とよぶ．特に，対称関数 f について，任意の $\boldsymbol{a}\succ\boldsymbol{b}$ となる $\mathbb{R}^d$ に値を持つ2つのベクトル $\boldsymbol{a},\boldsymbol{b}$ が $f(\boldsymbol{a})\ge f(\boldsymbol{b})$ を満たすとき，対称関数 f を **Schur 凸関数**とよぶ．$-f$ が Schur 凸関数のとき **Schur 凹関数**とよぶ．以下の補題より，Schur 凸関数，Schur 凹関数は凸関数，凹関数の一般化となる．

補題 2.3.3　対称関数 f が凸関数であるとき，Schur 凸関数となる．

証明.　$\boldsymbol{a}\succ\boldsymbol{b}$ とする．このとき，置換群 S_d 上の確率分布 p を適切に選ぶと $\sum_{g\in S_d} p(g)g(\boldsymbol{a})=\boldsymbol{b}$ が成り立つ．したがって，$f(\boldsymbol{b})\le\sum_{g\in S_d} p(g)f(g(\boldsymbol{a}))=f(\boldsymbol{a})$ となり題意を得る．□

また，以下の必要十分条件も知られている．

補題 2.3.4 [83, p.57]　対称関数 f が偏微分可能であるとき，f が Schur 凸関数となることと任意の i,j について $(x_i-x_j)(\frac{\partial f}{\partial x_i}-\frac{\partial f}{\partial x_j})\ge 0$ が成り立つことは同値である．

例 2.3.5　Schur 関数

$$\chi_{\boldsymbol{n}}(a_1,\ldots,a_d) := \frac{\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\prod_{l=1}^r a_l^{n_{\sigma(l)}+\delta_{\sigma(l)}}}{\prod_{j<l}(a_j-a_l)} \tag{2.12}$$

は定義域を $\mathbb{R}_+^d$ すると，$\boldsymbol{n}=(\underbrace{1,\ldots,1}_{n},0,\ldots,0)$ の場合の関数 $\chi_{\boldsymbol{n}}(a_1,\ldots,a_d)=\sum_{1\le i_1<\ldots<i_n\le d} a_{i_1}\cdots a_{i_n}$ は補題 2.3.4 より Schur 凹関数である．$\boldsymbol{n}=(n,0,\ldots,0)$ の場合の関数 $\chi_{\boldsymbol{n}}(a_1,\ldots,a_d)=\sum_{1\le i_1\le\ldots\le i_n\le d} a_{i_1}\cdots a_{i_n}$ は補題 2.3.4

よりSchur 凸関数である.

2.3.2 確率分布と不等式

次に確率分布とそれに従う確率変数 X が与えれたときに得られる不等式を紹介する. 期待値を E を用いて表すとすると, 凸関数の定義から以下の定理を得る.

補題 2.3.6 (Jensen の不等式) f を凸関数とすると不等式 $\mathrm{E}f(X) \geq f(\mathrm{E}X)$ が成り立つ.

ここで, エルミート行列 A のスペクトル分解 $A = \sum_i a_i E_i$ を考え, 実数値関数 f に対して $f(A)$ を $f(A) := \sum_i f(a_i) E_i$ で定義する. 量子状態 ρ から決まる確率分布 $\mathrm{Tr}\, E_i \rho$ に対して, 上の Jensen の不等式を適用すると, 実数上で定義された凸関数 f は以下を満たす.

$$\mathrm{Tr}\, \rho f(A) \geq f(\mathrm{Tr}\, \rho A). \tag{2.13}$$

さらに, 以下の不等式も成り立つ.

補題 2.3.7 (Markov の不等式) 非負の値をとる確率変数 X について, $\mathrm{P}\{X \geq a\} \leq \frac{\mathrm{E}X}{a}$ が成り立つ.

証明. 確率変数 X が離散型の場合のみ示す. 確率変数 X の実現値を x とすると, $\mathrm{P}\{X \geq a\} = \sum_{x:x \geq a} \mathrm{P}(x) \leq \sum_{x:x \geq a} \mathrm{P}(x) \frac{x}{a} \leq \sum_x \mathrm{P}(x) \frac{x}{a} = \frac{\mathrm{E}X}{a}$ となり題意を得る. □

2.3.3 Hölder の不等式とその周辺

一般の測度空間 Ω と測度 μ の組が与えられたとき, Ω 上の関数 f と実数 p に対して, p ノルム $\|f\|_p := (\int_\Omega |f(\omega)|^p \mu(d\omega))^{1/p} = \||f|^p\|_1^{1/p}$ を定義する. (p が負の数のときも含むとする.) $1/p + 1/q = 1$ を満たす実数 $\infty > p, q > 1$ を選ぶと, 非負値な実数 a, b は **Young の不等式**: $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$ を満たすことが知られている. $a = b$ のときのみ等号が成立する. この Young の不等式を用いると, $|fg(\omega)| \leq \frac{|f(\omega)|^p}{p} + \frac{|g(\omega)|^q}{q}$ が示せる. これを積分すると,

$$\|fg\|_1 \le \frac{\|f\|_p^p}{p} + \frac{\|g\|_q^q}{q} \tag{2.14}$$

を得る．特に，$c := \|g\|_q^{q/p}/\|f\|_p$ と置くと，$\|cf\|_p^p = \|g\|_q^q$ を満たす．したがって，Young の不等式の等号成立条件より，$\|cfg\|_1 \le \frac{\|cf\|_p^p}{p} + \frac{\|g\|_q^q}{q} = \|cf\|_p\|g\|_q$ を得る．両辺を c で割ることにより，$1/p+1/q=1$ を満たす実数 $\infty > p, q > 1$ についての **Hölder の不等式**を得る．

$$\|fg\|_1 \le \|f\|_p\|g\|_q. \tag{2.15}$$

逆に，$1/p+1/q=1$ を満たす実数 $1 > p > 0 > q$ については，以下の **Hölder の逆不等式**が示せる．

$$\|fg\|_1 \ge \|f\|_p\|g\|_q. \tag{2.16}$$

この不等式は，Hölder の不等式から以下のように示すことができる．$s := -\frac{1}{q}$ に対して，$p' := \frac{1+s}{s}$, $q' := 1+s$ と関数 $|fg|^{\frac{1}{1+s}}$, $|f|^{-\frac{1}{1+s}}$ に Hölder の不等式 (2.15) を適用すると，

$$\begin{aligned}\||fg|\|_1^{\frac{1}{1+s}} \||f|^{-\frac{1}{s}}\|_1^{\frac{s}{1+s}} &= \|(|fg|^{\frac{1}{1+s}})^{1+s}\|_1^{\frac{1}{1+s}} \|(|f|^{-\frac{1}{1+s}})^{\frac{1+s}{s}}\|_1^{\frac{s}{1+s}} \\ &\ge \||fg|^{\frac{1}{1+s}}|f|^{-\frac{1}{1+s}}\|_1 = \||g|^{\frac{1}{1+s}}\|_1\end{aligned}$$

となり，$\||fg|\|_1^{\frac{1}{1+s}} \ge \||g|^{\frac{1}{1+s}}\|_1 \||f|^{-\frac{1}{s}}\|_1^{-\frac{s}{1+s}}$ を得る．両辺を $1+s$ 乗することで，(2.16) を得る．

上記の議論を μ が確率測度であるとき，2つの確率変数 X, Y に適用する．$1/p + 1/q = 1$ を満たす実数 $\infty > p, q > 1$ について，(2.14) より，$\mathrm{E}|XY| \le \frac{\mathrm{E}X^p}{p} + \frac{\mathrm{E}X^q}{q}$ を得る．特に，$p = q = 2$ のとき，以下の補題を得る．

補題 2.3.8　2つの確率変数 X, Y について，$2\mathrm{E}XY \le 2\mathrm{E}|XY| \le \mathrm{E}X^2 + \mathrm{E}Y^2$ が成り立つ．すなわち，$\mathrm{E}(X+Y)^2 \le 2\mathrm{E}X^2 + 2\mathrm{E}Y^2$ が成り立つ．

次は，上記の議論を数列空間の場合に適用する．Hölder の不等式と Hölder の逆不等式から2つの数列 $\{a_j\}_{j=1}^k$, $\{b_j\}_{j=1}^k$ は

$$\sum_{j=1}^k |a_j b_j| \le \left(\sum_{j=1}^k |a_j|^p\right)^{1/p} \left(\sum_{j=1}^k |b_j|^q\right)^{1/q}, \quad \frac{1}{p} + \frac{1}{q} = 1,\ \infty > p, q > 1$$

$$\sum_{j=1}^{k} |a_j b_j| \geq \left(\sum_{j=1}^{k} |a_j|^p\right)^{1/p} \left(\sum_{j=1}^{k} |b_j|^q\right)^{1/q}, \quad \frac{1}{p}+\frac{1}{q}=1,\ 1>p>0>q$$

を満たす．ある実数 s が与えられたとき，確率分布 $\{p_j\}$ とある数列 $\{a_j\}$ が与えれた場合に上記の式を代入すると以下を得る．

$$\sum_{j=1}^{k} |p_j^s a_j| \geq \left(\sum_{j=1}^{k} |a_j|^p\right)^{1/p} \left(\sum_{j=1}^{k} p_j^{sq}\right)^{1/q} = \left(\sum_{j=1}^{k} |a_j|^{\frac{1}{1-s}}\right)^{1-s}, \quad 0>s \tag{2.17}$$

$$\sum_{j=1}^{k} |p_j^s a_j| \leq \left(\sum_{j=1}^{k} |a_j|^p\right)^{1/p} \left(\sum_{j=1}^{k} p_j^{sq}\right)^{1/q} = \left(\sum_{j=1}^{k} |a_j|^{\frac{1}{1-s}}\right)^{1-s}, \quad 1>s>0 \tag{2.18}$$

$$\sum_{j=1}^{k} |p_j^s a_j| \geq \left(\sum_{j=1}^{k} |a_j|^q\right)^{1/q} \left(\sum_{j=1}^{k} p_j^{sp}\right)^{1/p} = \left(\sum_{j=1}^{k} |a_j|^{\frac{1}{1-s}}\right)^{1-s}, \quad s>1. \tag{2.19}$$

ここで，(2.17), (2.18) では，$q=\frac{1}{s}$ とし，(2.19) では，$p=\frac{1}{s}$ とした．

2.3.4 行列版への拡張

上記の議論を行列版に拡張することがよく知られている．実数の部分集合で定義された関数 f が以下を満たすとき，**作用素凸関数**という：f の定義域に固有値を持つエルミート行列 A, B と $1>\lambda>0$ に対して，$\lambda f(A)+(1-\lambda)f(B) \geq f(\lambda A+(1-\lambda)B)$ が成り立つ．関数 $-f$ が作用素凸関数のとき，f は**作用素凹関数**という．作用素凸関数は以下に定義する作用素単調関数と密接な関係にある．実数の部分集合で定義された関数 f が以下を満たすとき，**作用素単調**という．f の定義域に固有値を持つエルミート行列 A, B が $A \geq B$ を満たすとき，$f(A) \geq f(B)$ が成り立つ．さらに，以下の定理が知られている [59, 58].

定理 2.3.9 $[0,\infty)$ で定義された関数 f について以下は同値である．

(1) f は作用素単調関数である．

(2) $t/f(t)$ は作用素単調関数である．

(3)　f は作用素凹関数である．

例えば，$1 > s > 0$ について $x \mapsto -x^{-s}$, $x \mapsto x^s$, $x \mapsto \log x$, $x \mapsto -x^{1+s}$, $x \mapsto x \log x$ は作用素単調関数かつ作用素凹関数である．$x \mapsto x^{1+s}$, $x \mapsto x^{-s}$ $x \mapsto x \log x$ は作用素凸関数である．

さらに，作用素凸関数について以下の定理が知られている [59, 58]．

定理 2.3.10　$[0, \infty)$ で定義された関数 f について以下は同値である．

(1)　f は作用素凸関数である．

(2)　$C^\dagger C \le I$ となる行列 C と f の定義域に固有値を持つエルミート行列 A について $f(C^\dagger AC) \le C^\dagger f(A)C$ が成り立つ．

(3)　行列の組 $C_1, \ldots, C_k$ が $\sum_j C_j^\dagger C_j = I$ を満たすとする．f の定義域に固有値を持つエルミート行列 A について $f(\sum_j C_j^\dagger AC_j) \le \sum_j C_j^\dagger f(A)C_j$ が成り立つ．

また，行列のトレースについて以下の定理が知られている [59, 7, 58]．

定理 2.3.11（Golden-Thompson）　2つのエルミート行列 A, B は以下を満たす．

$$\mathrm{Tr}\, e^{A+B} \le \mathrm{Tr}\, e^A e^B. \tag{2.20}$$

行列 A と実数 p に対して p ノルムを $\|A\|_p := \||A|^p\|_1^{1/p}$ で定義する．このとき，Hölder の不等式については以下の作用素版が知られている [59, 58]．

定理 2.3.12（作用素版 Hölder の不等式）　$1/p+1/q = 1$ を満たす実数 $\infty > p, q > 1$ を選ぶ．2つの行列 A, B は以下を満たす．

$$\|AB\|_1 \le \|A\|_p \|B\|_q. \tag{2.21}$$

この定理を用いて以下の作用素版 Hölder の逆不等式を示すことができる．

定理 2.3.13（作用素版 Hölder の逆不等式）　$1/p + 1/q = 1$ を満たす実数 $1 > p > 0 > q$ を選ぶ．2つの半正定値行列 $A, B \ge 0$ は以下を満たす．

$$\|AB\|_1 \ge \|A\|_p \|B\|_q. \tag{2.22}$$

証明.　A, B が可逆の場合について示す．固有値 0 を持つ場合は，上記の場合の極限を考えることで得られる．$a := \log A$, $b := \log B$ とする．さらに，$s := -\frac{1}{q}$ に対して，$p' := \frac{1+s}{s}$, $q' := 1+s$ と行列 $(e^{a+b})^{\frac{1}{1+s}}$, $(e^{a})^{-\frac{1}{1+s}}$ に作用素版 Hölder の不等式 (2.21) を適用すると，

$$\|e^{a+b}\|_1^{\frac{1}{1+s}} \|e^{-\frac{a}{s}}\|_1^{\frac{s}{1+s}} = \|(e^{\frac{a+b}{1+s}})^{1+s}\|_1^{\frac{1}{1+s}} \|(e^{-\frac{a}{1+s}})^{\frac{1+s}{s}}\|_1^{\frac{s}{1+s}}$$
$$\geq \|e^{\frac{a+b}{1+s}} e^{-\frac{a}{1+s}}\|_1 \geq \|e^{\frac{b}{1+s}}\|_1$$

を得る．最後の不等式では (2.20) を用いた．したがって，$\|e^{a+b}\|_1^{\frac{1}{1+s}} \geq \|e^{\frac{b}{1+s}}\|_1 \|e^{-\frac{a}{s}}\|_1^{-\frac{s}{1+s}}$ を得る．両辺を $1+s$ 乗し，(2.20) から得られる不等式 $\|e^a e^b\|_1 \geq \|e^{a+b}\|_1$ に注意すると，(2.22) を得る．　□

したがって，実数 s と非負定値行列 A と密度行列 ρ について (2.17), (2.18), (2.19) と同じように作用素版 Hölder の不等式 (2.21) と作用素版 Hölder の逆不等式 (2.22) を用いると，以下の不等式を得る．

$$\|\rho^s A\|_1 \geq \|A\|_{\frac{1}{1-s}}, \quad 0 > s \tag{2.23}$$

$$\|\rho^s A\|_1 \leq \|A\|_{\frac{1}{1-s}}, \quad 1 > s > 0 \tag{2.24}$$

$$\|\rho^s A\|_1 \geq \|A\|_{\frac{1}{1-s}}, \quad s > 1. \tag{2.25}$$

2.4　量子系での情報量

2.4.1　情報源の持つ情報量

量子情報では，系 $\mathcal{H}$ が状態 ρ にあるときの系の持つ情報の量を測るために，ρ の関数として情報量を定義することが多い．情報量は先に議論した凸性や凹性を満たすことが多いが，これらの性質に加え，以下の性質にも注目する．

加法性：　関数 $f(\rho)$ が $f(\rho_1 \otimes \rho_2) = f(\rho_1) + f(\rho_2)$ を満たすとき加法性を満たすという．

情報量の中で最も重要なのが，以下に定義する **von Neumann エントロピー**である．

$$H(\rho) := -\operatorname{Tr} \rho \log \rho. \tag{2.26}$$

von Neumann エントロピー $H(\rho)$ の値が大きいほど，ランダムの度合いが大きいと考える．von Neumann エントロピー $H(\rho)$ は6.6節で述べるように，情報源圧縮の際の圧縮限界を表す量として現れる．von Neumann エントロピー以外にも，ランダムな度合いを表す量として $\psi(s|\rho) := \log \operatorname{Tr} \rho^{1-s}$ が知られている．この量を用いて，$1-s$ 次の **Rényi エントロピー**：$H_{1-s}(\rho) := \frac{\psi(s|\rho)}{s}$ が定義される．$s \to 0$ の極限を考えることで，von Neumann エントロピー $H(\rho) = \lim_{s\to 0} H_{1-s}(\rho)$ が得られる．Rényi エントロピー $H_{1-s}(\rho)$ は値が大きいほど，ランダムな度合いが大きい．

後の系2.6.4で述べるように，von Neumann エントロピー $H(\rho)$ は凹性を満たし，$e^{\psi(s|\rho)}$ は $s<0$ のとき凸性を満たし，$0<s<1$ のとき凹性を満たす．さらに，min-エントロピー $H_{\min}(\rho) := -\log \|\rho\|$，max-エントロピー $H_{\max}(\rho) := \log \operatorname{rank} \rho$ を以下で定義する．これらの値は以下のようにRényi エントロピーの極限として与えられる．

$$H_{\min}(\rho) = \lim_{s\to -\infty} H_{1-s}(\rho), \quad H_{\max}(\rho) = \lim_{s\to 1} H_{1-s}(\rho).$$

$s \neq 0$ について，$\psi(s|\rho)$ の2階微分は以下のように計算できる．

$$\psi''(s|\rho) = \frac{\operatorname{Tr}(\log \rho)^2 \rho^s \operatorname{Tr} \rho^s - (\operatorname{Tr}(\log \rho)\rho^s)^2}{(\operatorname{Tr} \rho^s)^2} > 0. \tag{2.27}$$

したがって，関数 $s \mapsto \psi(s|\rho)$ は凸関数であることが確認できる．さらに，$\psi(0|\rho) = 0$ であるので，$H_{1-s}(\rho) = \frac{\psi(s|\rho)}{s}$ は s の関数として，単調増加となる．したがって，$s_1 < 0, 0 < s_2 < 1$ に対して

$$H_{\min}(\rho) \le H_{1-s_1}(\rho) \le H(\rho) \le H_{1-s_2}(\rho) \le H_{\max}(\rho)$$

を得る．$H_{\max}(\rho)$ は定義から明らかであるように凹性を満たす．von Neumann エントロピー，Rényi エントロピー，min-エントロピー，max-エントロピーは加法性を満たす．

なお，合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の純粋状態 $|\Phi\rangle\langle\Phi|$ が与えられ，$\rho_A = \operatorname{Tr}_B |\Phi\rangle\langle\Phi|$，$\rho_B = \operatorname{Tr}_A |\Phi\rangle\langle\Phi|$ となるとき，2つの密度行列の固有値のうち，0でないもの

については一致する．したがって，ρ_A についての上記の全ての情報量は ρ_B についての情報量に一致する．

さらに，確率分布 $\boldsymbol{p} = (p_1, \ldots, p_k)$ に対しても，$\rho(\boldsymbol{p})$ を用いて，**Shannon エントロピー** $H(\boldsymbol{p}) := H(\rho(\boldsymbol{p}))$, $\psi(s|\boldsymbol{p}) := \psi(s|\rho(\boldsymbol{p}))$ などが定義される．

そして，$\dim \mathcal{H} = d$ のとき，von Neumann エントロピーの凹性より，$H(\rho) \le \log d$ が成り立つ．さらに，$\phi''(0|\rho)$ には $\operatorname{Tr} \rho \log \rho^2$ が現れるが，$d = 2$ のときは，

$$\max_{\operatorname{Tr}\rho=1} \operatorname{Tr} \rho \log \rho^2 = \frac{1-\sqrt{1-4/e^2}}{2}\left(\log \frac{1-\sqrt{1-4/e^2}}{2}\right)^2 + \frac{1+\sqrt{1-4/e^2}}{2}\left(\log \frac{1+\sqrt{1-4/e^2}}{2}\right)^2$$

となり，$d \ge 3$ のときは

$$\max_{\operatorname{Tr}\rho=1} \operatorname{Tr} \rho \log \rho^2 = (\log d)^2 \tag{2.28}$$

となる．$d = 2$ の場合については計算により確認でき，$d \ge 3$ の場合は以下のように示せる．

(2.28) の証明.　$d = 3$ の場合，(2.28) は計算により確認できる．$d \ge 4$ の場合について (2.28) を帰納法により示す．(2.28) の左辺を a_d とする．すると，$a_d \ge (\log d)^2$ が成り立つ．さらに，帰納法の仮定より，$a_d = \sum_{i=1}^{d} p_i (\log p_i)^2$ かつ $p_i > 0$ $(i = 1, \ldots, d)$ となる ρ の固有値 $\{p_i\}$ が存在する．

ここで，Lagrange 未定乗数法を用いる．λ' を Lagrange 未定乗数とすると，$(\log p_i)^2 + 2 \log p_i - \lambda' = 0$ を得る．$\lambda := \sqrt{1+\lambda'}$ とすると，解は $\log p_i = -1 \pm \lambda$ となる．そのため，p_i の順序を入れ替えることにより，以下を満たす $0 \le r \le d$ が存在する．

$$\log p_i = \begin{cases} -1 + \lambda & \text{if } r \ge i \\ -1 - \lambda & \text{if } r < i. \end{cases}$$

$\sum_i p_i = 1$ であるから，$1 = r e^{-1+\lambda} + (d-r) e^{-1-\lambda}$ となり，$x := e^{\lambda}$ は $rx^2 - ex + d - r = 0$ を満たす．判別式が 0 よりも大きいため，$e^2 - 4r(d-r) \ge 0$

を得る．これを解くと $r \le \frac{d-\sqrt{d^2-e^2}}{2}$, $\frac{d+\sqrt{d^2-e^2}}{2} \le r$ を得る．関数 $c(x) := \frac{x-\sqrt{x^2-e^2}}{2}$ は (e,∞) において単調減少であり，$c(4) < 1$ となる．したがって，上述の r についての不等式より，r は 0 または d と一致する．したがって，$p_i = 1/d$ となり (2.28) を得る．□

2.4.2　2つの情報源の相違度

系 $\mathcal{H}$ 上の2つの密度行列 ρ_1, ρ_2 がどの程度離れているかを測る尺度が複数提案されている．このような2つの密度行列 ρ_1, ρ_2 の相違の度合いを表す関数 $f(\rho_1,\rho_2)$ に対して，以下の性質を考える．

接合凸性：　関数 $f(\rho_1,\rho_2)$ が $\lambda f(\rho_1,\rho_2)+(1-\lambda)f(\rho_1',\rho_2') \ge f(\lambda\rho_1+(1-\lambda)\rho_1', \lambda\rho_2+(1-\lambda)\rho_2')$ を満たすとき，接合凸性を満たすという．

加法性：　関数 $f(\rho_1,\rho_2)$ が $f(\rho_1\otimes\rho_1', \rho_2\otimes\rho_2') = f(\rho_1,\rho_2)+f(\rho_1',\rho_2')$ を満たすとき加法性を満たすという．

擬平方距離：　$\mathcal{S}(\mathcal{H})$ の1次元部分集合（曲線）$\{\rho_t \mid t\in\mathbb{R}\}$ に対して適切にパラメータをとると以下が成り立つとき，関数 $f(\rho_1,\rho_2)$ は擬平方距離であるという．任意の t に対して $f(\rho_t,\rho_{t+\epsilon}) = c_t\epsilon^2 + o(\epsilon^2)$ を満たす c_t がとれる．

一般に，距離の二乗で $f(\rho_1,\rho_2)$ が与えられる場合，$f(\rho_1,\rho_2)$ は擬平方距離となる．

以下，2つの密度行列 ρ_1, ρ_2 の相違の度合いを表す尺度の例を見ていく．1つ目はトレースノルムを用いるもので，**トレースノルム距離** $d_1(\rho_1,\rho_2) := \frac{1}{2}\|\rho_1-\rho_2\|_1$ である．2つ目は，**忠実度**とよばれるもので，$F(\rho_1,\rho_2) := \mathrm{Tr}\,|\sqrt{\rho_1}\sqrt{\rho_2}|$ で与えられる．片方が純粋状態のときは忠実度の二乗は $\mathrm{Tr}\,\rho_1\rho_2$ に一致する．この値を用いて，**擬忠実度**：$\tilde{F}(\rho_1,\rho_2) := \mathrm{Tr}\,\rho_1\rho_2$ を定義する．これらの値を変形して，**対数逆平方忠実度** $F_{\log}(\rho_1,\rho_2) := -2\log\mathrm{Tr}\,|\sqrt{\rho_1}\sqrt{\rho_2}|$, **対数逆擬忠実度** $\tilde{F}_{\log}(\rho_1,\rho_2) := -\log\mathrm{Tr}\,\rho_1\rho_2$ を定義する．忠実度を用いて，**Bures の距離** $b(\rho_1,\rho_2)^2 := 1-\mathrm{Tr}\,|\sqrt{\rho_1}\sqrt{\rho_2}|$ が定義できる．トレースノルム距離，Bures の距離は，距離の公理を満たす．また，上述の情報量を変形して，2つの密度行列 ρ_1, ρ_2 の相違の度合いを測ることもできる．von Neumann エントロピーの下に，**相対エントロピー** $D(\rho_1\|\rho_2) := \mathrm{Tr}\,\rho_1(\log\rho_1-\log\rho_2)$ を定義する．先と

同様に，$\psi(s|\rho_1\|\rho_2) := \log \mathrm{Tr}\, \rho_1^{1-s}\rho_2^s$ を定義する．この関数を用いて，$1-s$ 次の**相対 Rényi エントロピー** $D_{1-s}(\rho_1\|\rho_2) := -\frac{\psi(s|\rho_1\|\rho_2)}{s}$ を定義する．$s \to 0$ の極限を考えることで，相対エントロピー $D(\rho_1\|\rho_2) = \lim_{s\to 0} D_{1-s}(\rho_1\|\rho_2)$ が得られる．さらに，相対 Rényi エントロピー $D_{1-s}(\rho_1\|\rho_2)$ の値が大きいほど 2 つの状態は離れている．$s = 1/2$ のとき，$e^{\psi(s|\rho_1\|\rho_2)}$ は忠実度 $F(\rho_1, \rho_2)$ と類似しているが，異なる量である．一般には，

$$F(\rho_1, \rho_2) = \mathrm{Tr}\, |\sqrt{\rho_1}\sqrt{\rho_2}| \geq \mathrm{Tr}\, \sqrt{\rho_1}\sqrt{\rho_2} = e^{\psi(1/2|\rho_1\|\rho_2)} \tag{2.29}$$

である．ρ_1 と ρ_2 が可換であるとき等号が成り立つ．さらに，**相対 min-エントロピー** $D_{\min}(\rho_1\|\rho_2) := -\log \mathrm{Tr}\, \rho_2 P(\rho_1)$，**相対 max-エントロピー** $D_{\max}(\rho_1\|\rho_2) := \log \|\rho_2^{-\frac{1}{2}}\rho_1\rho_2^{-\frac{1}{2}}\|$ を以下で定義する．（min-エントロピー，max-エントロピーの場合と比べて max と min が逆転していることに注意せよ．）ここで，$P(\rho)$ は ρ の値域への射影である．$D_{\min}(\rho_1\|\rho_2)$ は相対 Rényi エントロピーの極限として $D_{\min}(\rho_1\|\rho_2) = \lim_{s\to 1} D_{1-s}(\rho_1\|\rho_2)$ で与えられる．一方，$D_{\max}(\rho_1\|\rho_2)$ は $\|\rho_2^{-\frac{1}{2}}\rho_1\rho_2^{-\frac{1}{2}}\| = \|\rho_1^{\frac{1}{2}}\rho_2^{-1}\rho_1^{\frac{1}{2}}\|$ を満たす．また，この値は $\lambda\rho_2 \geq \rho_1$ を満たす最小の実数 λ である．さらに，$\mathrm{Tr}\, \rho_1(\rho_1^{\frac{1}{2}}\rho_2^{-1}\rho_1^{\frac{1}{2}}) \leq \|\rho_1^{\frac{1}{2}}\rho_2^{-1}\rho_1^{\frac{1}{2}}\|$ となることから，

$$D_{-1}(\rho_1\|\rho_2) = \log \mathrm{Tr}\, \rho_1(\rho_1^{\frac{1}{2}}\rho_2^{-1}\rho_1^{\frac{1}{2}}) \leq \log \|\rho_1^{\frac{1}{2}}\rho_2^{-1}\rho_1^{\frac{1}{2}}\| = D_{\max}(\rho_1\|\rho_2)$$

を得る．関数 $s \mapsto \psi(s|\rho_1\|\rho_2)$ は凸関数となる．そのため，$\psi(0|\rho_1\|\rho_2) = 0$ であることに注意すると，$D_{1-s}(\rho_1\|\rho_2) := \frac{-\psi(s|\rho_1\|\rho_2)}{s}$ は s に関して単調減少となる．したがって，$-1 \leq s_1 < 0,\ 0 < s_2 < 1$ について

$$D_{\min}(\rho_1\|\rho_2) \leq D_{s_2}(\rho_1\|\rho_2) \leq D(\rho_1\|\rho_2) \leq D_{s_1}(\rho_1\|\rho_2) \leq D_{\max}(\rho_1\|\rho_2) \tag{2.30}$$

を得る．

後の系 2.6.3 で述べるように，トレースノルム距離，Bures の距離の二乗，相対エントロピー，相対 min-エントロピー，$-1 < s < 0$ のときの $e^{\psi(s|\rho_1\|\rho_2)}$ は全て，接合凸性を満たす．他に，$1 > s > 0$ のとき，$-e^{\psi(s|\rho_1\|\rho_2)}$ や $-F(\rho_1, \rho_2)$ も接合凸性を満たす．また，忠実度の二乗 $F(\rho_1, \rho_2)^2$ は ρ_1 または ρ_2 について凸性を満たす．また，相対エントロピー，相対 Rényi エントロピー，相対

min-エントロピー，相対 max-エントロピー対数逆平方忠実度，対数逆擬忠実度は加法性を満たす．そして，相対エントロピー，相対 Rényi エントロピー，相対 min-エントロピー，相対 max-エントロピーは擬平方距離となる．

さらに，2つの確率分布 $\boldsymbol{p} = (p_1, \ldots, p_k)$，$\boldsymbol{q} = (p_1, \ldots, p_k)$ に対しても，それらを対角成分に持つ対角行列 $\rho(\boldsymbol{p})$，$\rho(\boldsymbol{q})$ を用いて，**相対エントロピー** $D(\boldsymbol{p}\|\boldsymbol{q}) := D(\rho(\boldsymbol{p})\|\rho(\boldsymbol{q}))$ などが定義される．

ここで，$X = \sum_i x_i E_i$ についてのピンチング $\Lambda_X(\rho) = \sum_i E_i \rho E_i$ の前後でどれだけ状態が異なるかについて，以下の式が成り立つ．

$$D(\rho\|\Lambda_X(\rho)) = H(\Lambda_X(\rho)) - H(\rho). \tag{2.31}$$

特に，トレースノルム距離については $\|(I-E_i)\rho\|_1 = \mathrm{Tr}(I-E_i)\rho U$, $\|E_i\rho(I-E_i)\|_1 = \mathrm{Tr}\, E_i\rho(I-E_i)U'$ を満たすユニタリ U, U' が存在するので，Schwarz の不等式を用いることで，以下が成り立つ．

$$\begin{aligned}
&\|\rho - E_i\rho E_i\|_1 = \|(I-E_i)\rho + E_i\rho(I-E_i)\|_1 \\
&\quad = \|(I-E_i)\rho\|_1 + \|E_i\rho(I-E_i)\|_1 = \mathrm{Tr}(I-E_i)\rho U + \mathrm{Tr}\, E_i\rho(I-E_i)U' \\
&\quad \le \sqrt{\mathrm{Tr}(I-E_i)\rho(I-E_i) \quad \mathrm{Tr}\, U^\dagger \rho U} \\
&\qquad + \sqrt{\mathrm{Tr}\, E_i\rho E_i\, \mathrm{Tr}\, U'^\dagger (I-E_i)\rho(I-E_i)U'} \\
&\quad = \sqrt{\mathrm{Tr}(I-E_i)\rho} + \sqrt{\mathrm{Tr}\, E_i\rho\, \mathrm{Tr}(I-E_i)\rho} \le 2\sqrt{\mathrm{Tr}(I-E_i)\rho}.
\end{aligned} \tag{2.32}$$

したがって，

$$\begin{aligned}
&\|\rho - \Lambda_X(\rho)\|_1 = \|(\rho - E_i\rho E_i) + \sum_{j\neq i} E_j\rho E_j\|_1 \le \|\rho - E_i\rho E_i\| + \mathrm{Tr} \sum_{j\neq i} E_j\rho E_j \\
&\quad \le \sqrt{\mathrm{Tr}(I-E_i)\rho} + \sqrt{\mathrm{Tr}\, E_i\rho\, \mathrm{Tr}(I-E_i)\rho} + \mathrm{Tr}(I-E_i)\rho \le 3\sqrt{\mathrm{Tr}(I-E_i)\rho}
\end{aligned} \tag{2.33}$$

を得る．

2.4.3　2つの系の相関

さらに，2つの系 $\mathcal{H}_A, \mathcal{H}_B$ の合成系 $\mathcal{H}\otimes\mathcal{K}$ 上の状態 ρ に対して，この相関を表す量として，**相互情報量** $I_\rho(A:B) := H(\rho_A) + H(\rho_B) - H(\rho)$ を定義す

る．この値は，演習問題3で扱うように，$D(\rho\|\rho_A\otimes\rho_B)$ と等しい．したがって，$I_\rho(A:B)$ は状態が ρ であるとき，独立である場合から離れている度合いを表す量と見なすことができる．そのため，$I_\rho(A:B)$ は状態が ρ であるときの相関を表す量として用いられる．

相互情報量と関連して相対エントロピーについては，いくつか重要な公式があるので，ここで紹介する．合成系上の状態 ρ と任意のテンソル積状態 $\sigma_A\otimes\sigma_B$ との相対エントロピーに注目しよう．すると，

$$
\begin{aligned}
D(\rho\|\sigma_A\otimes\sigma_B) &= \operatorname{Tr}\rho(\log\rho-\log\sigma_A\otimes\sigma_B)\\
&= \operatorname{Tr}\rho(\log\rho-(\log\sigma_A)\otimes I_B - I_A\otimes(\log\sigma_B))\\
&= \operatorname{Tr}\rho(\log\rho-(\log\rho_A)\otimes I_B - I_A\otimes(\log\rho_B))\\
&\quad + \operatorname{Tr}\rho((\log\rho_A)\otimes I_B + I_A\otimes(\log\rho_B) - (\log\sigma_A)\otimes I_B - I_A\otimes(\log\sigma_B))\\
&= \operatorname{Tr}\rho(\log\rho-\log(\rho_A\otimes\rho_B))\\
&\quad + \operatorname{Tr}\rho_A(\log\rho_A-\log\sigma_A) + \operatorname{Tr}\rho_B(\log\rho_B-\log\sigma_B)\\
&= D(\rho\|\rho_A\otimes\rho_B) + D(\rho_A\|\sigma_A) + D(\rho_B\|\sigma_B)\\
&= D(\rho\|\rho_A\otimes\rho_B) + D(\rho_A\otimes\rho_B\|\sigma_A\otimes\sigma_B) \qquad (2.34)
\end{aligned}
$$

となる．特に，$\sigma_A=\rho_A$ の場合は

$$
D(\rho\|\rho_A\otimes\sigma_B) = D(\rho\|\rho_A\otimes\rho_B) + D(\rho_B\|\sigma_B) \qquad (2.35)
$$

となる．この事実は，Pythagoras 型の定理とよばれ以下のような意味がある．テンソル積で書ける密度行列の空間 S を考える．任意の密度行列 ρ から空間 S 上の点 $\sigma_A\otimes\sigma_B$ への相対エントロピー $D(\rho\|\sigma_A\otimes\sigma_B)$ は空間 S の中で相対エントロピーの意味で最も近い点 $\rho_A\otimes\rho_B$ への相対エントロピー $D(\rho\|\rho_A\otimes\rho_B)$ と $\rho_A\otimes\rho_B$ から $\sigma_A\otimes\sigma_B$ への相対エントロピー $D(\rho_A\otimes\rho_B\|\sigma_A\otimes\sigma_B)$ の和で表される．いわば，図2.1で示すように，$\rho_A\otimes\rho_B$ は ρ から空間 S への垂線の足となる．この事実から

$$
D(\rho\|\sigma_A\otimes\sigma_B) \ge D(\rho\|\rho_A\otimes\rho_B) \qquad (2.36)
$$

が示せる．

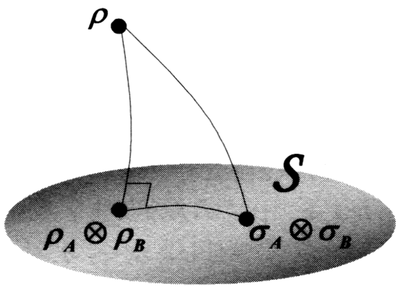


図 2.1　Pythagoras 型の定理

量子通信では，$\mathcal{H}_A$ が古典系 $\mathcal{X} := \{1, \ldots, k\}$ である場合，通信路は $x \in \mathcal{X}$ に応じて決まる $\mathcal{H}_B$ 上の密度行列 $W(x)$ によって与えられる．6.7 節で詳しく述べるように，写像 $x \mapsto W(x)$ は古典-量子通信路とよばれる．このとき，合成系上の状態 $\sum_{x=1}^k p(x)|x\rangle\langle x| \otimes W(x)$ の相互情報量に注目することが多い．この値は，**量子伝送情報量**とよばれ，

$$
\begin{aligned}
I(p:W) &= H\left(\sum_{x=1}^k p(x)W(x)\right) - \sum_{x=1}^k p(x)H(W(x)) \\
&= \sum_{x=1}^k p(x)D\left(W(x)\middle\|\sum_{x=1}^k p(x)W(x)\right)
\end{aligned}
\tag{2.37}
$$

と一致する．von Neumann エントロピーの凹性より，ここで定義した $I(P:\rho)$ は確率分布 P について，凹関数となる．また，上記の不等式 (2.35) を適用すると，任意の $\mathcal{H}_B$ 上の密度行列 σ について

$$
\sum_{x=1}^k p(x)D(W(x)\|\sigma) = \sum_{x=1}^k p(x)D\left(W(x)\middle\|\sum_{x=1}^k p(x)W(x)\right) + D\left(\sum_{x=1}^k p(x)W(x)\middle\|\sigma\right)
\tag{2.38}
$$

を得る．

ここで，コンパクト群 G の $\mathcal{H}_B$ 上のユニタリ表現 f が与えられた場合を考えよう．そして，σ_B が f に関して不変，すなわち，$g \in G$ について，$\mathsf{f}(g)\sigma_B = \sigma_B\mathsf{f}(g)$ とする．このとき，任意の密度行列 ρ について，$D(\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger\|\sigma) = D(\rho\|\sigma)$ となることから，μ_G を不変測度とし，$\overline{\rho} := \int_G \mathsf{f}(g)\rho\mathsf{f}(g)^\dagger\mu_G(dg)$ とすると，$\overline{\rho}$ も f に関して不変であるから，

$$\begin{aligned} D(\rho\|\sigma) &= \int_G D(\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger\|\sigma)\mu_G(dg) \\ &= \int_G D(\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger\|\overline{\rho})\mu_G(dg) + D(\overline{\rho}\|\sigma) \\ &= D(\rho\|\overline{\rho}) + D(\overline{\rho}\|\sigma) = H(\overline{\rho}) - H(\rho) + D(\overline{\rho}\|\sigma) \end{aligned} \tag{2.39}$$

を得る．この事実は，以下に述べるように，先に述べた Pythagoras 型の定理の群不変版と見なすことができる．f に関して不変な密度行列の空間 S を考える．任意の密度行列 ρ から空間 S 上の点 σ への相対エントロピー $D(\rho\|\sigma)$ は，空間 S の中で相対エントロピーの意味で最も近い点 $\overline{\rho}$ への相対エントロピー $D(\rho\|\overline{\rho})$ と $\overline{\rho}$ から σ への相対エントロピー $D(\overline{\rho}\|\sigma)$ の和で表される．いわば，図 2.1 で示した場合と同じように，$\overline{\rho}$ は ρ から空間 S への垂線の足となる．なお，PVM $E = \{E_j\}_{j=1}^n$ に対して，群 $\mathbb{R}^n$ の表現 $\mathsf{f}(\theta_1, \ldots, \theta_n) := \sum_{j=1}^n e^{i\theta_j} E_j$ を考えると，PVM E のピンチング Λ_E は $\Lambda_E(\rho) = \overline{\rho}$ を満たす．すなわち，ρ のピンチング Λ_E の像は上記の表現に関して不変な状態の中で，相対エントロピーの意味で ρ に最も近い点である．

演習問題 3 $I_\rho(A:B) = D(\rho\|\rho_A \otimes \rho_B)$ を示せ．

演習問題 4 $\mathcal{H}$ の密度行列 ρ の任意の固有値 λ が以下を満たすことを示せ．

$$H(\rho) \le (1-\lambda)\log\dim\mathcal{H} + h(\lambda). \tag{2.40}$$

ただし，$h(x) := -x\log x - (1-x)\log(1-x)$ である．

2.4.4 量子通信路と情報量

次に，量子通信路の持つ情報量を先に与えた情報量を用いて記述する．入出力系がともに $\mathcal{H}$ である量子通信路 Λ がどれだけ正確に量子状態を伝送するか表す量として，エンタングルメント忠実度を導入しよう．入力系上の状態 ρ を考え，系 $\mathcal{H}$ と同じ次元の参照系 $\mathcal{H}_R$ を準備し，合成系 $\mathcal{H}\otimes\mathcal{H}_R$ 上の状態として，状態 ρ の純粋状態化 $|\Phi\rangle$ を考える．このとき，**エンタングルメント忠実度**を $F_e^2(\rho,\Lambda) := \langle\Phi|(\Lambda\otimes id)(|\Phi\rangle\langle\Phi|)|\Phi\rangle$ で定義する [102]．この値は，純粋状態化 $|\Phi\rangle$ の選び方に依存しないことに注意せよ．Λ の Kraus 表現 $\{F_m\}$ を用いると，

$$F_e^2(\rho,\Lambda) = \sum_m |\operatorname{Tr} F_m \rho|^2 \tag{2.41}$$

と書ける．ここで，関数 $\rho \mapsto |\operatorname{Tr} F_m \rho|^2$ が凸関数であることに注意すると，$F_e^2(\rho,\Lambda)$ は ρ の関数として凸となる．特に，ρ が純粋状態であるときは $F_e^2(\rho,\Lambda)$ は忠実度の二乗 $F(\rho,\Lambda(\rho))^2$ に一致する．そのため，$\rho = \sum_j p_j |x_j\rangle\langle x_j|$ であるとき，以下が成り立つ．

$$F_e^2(\rho,\Lambda) \le \sum_j p_j \langle x_j|\Lambda(|x_j\rangle\langle x_j|)|x_j\rangle. \tag{2.42}$$

特に，ρ が完全混合状態であるときは，$F_e^2(\rho,\Lambda)$ を $F_e^2(\Lambda)$ と略記する．$\mathcal{H} = \mathbb{C}^r$ であり，Θ が $\mathcal{H}$ 上の純粋状態の集合であるとき，Lie 群 $\mathrm{SU}(r)$ の等質空間としての不変測度 μ_Θ について

$$\frac{r}{r+1}(1 - F_e^2(\Lambda)) = 1 - \int_\Theta \langle\theta|\Lambda(|\theta\rangle\langle\theta|)|\theta\rangle \mu_\Theta(d\theta)$$

が成り立つ [38, (8.25)]．この事実は，量子通信路 Λ を用いて，純粋状態を伝送したとき，平均的な性能が量子通信路のエンタングルメント忠実度 $F_e^2(\Lambda)$ で与えられることを示している．それゆえ，エンタングルメント忠実度を評価することで，通信路の性能が評価できる．

次に，量子通信路がどの程度のコヒーレンスを保持しているか表す量として，**コヒーレント情報量** $I_c(\rho,\Lambda) := H(\Lambda(\rho)) - H(\Lambda \otimes id_R(|\Phi\rangle\langle\Phi|))$ を導入する [103]．ここで，状態 ρ の純粋状態化 $|\Phi\rangle$ である．この量は量子通信路 Λ の出力系 $\mathcal{H}_B$ が入力系 $\mathcal{H}_A$ と異なる場合でも定義され，純粋状態化 $|\Phi\rangle$ のとり方に依存しない．ここで Λ の Stinespring 表現 U を考えると，$U \otimes I(|\Phi\rangle\langle\Phi|)U^\dagger \otimes I$ は $\Lambda \otimes id_R(|\Phi\rangle\langle\Phi|)$ の純粋状態化となり，$\operatorname{Tr}_{B,R} U \otimes I(|\Phi\rangle\langle\Phi|)U^\dagger \otimes I = \operatorname{Tr}_B U\rho U^\dagger = \Lambda_E(\rho)$ となる．すなわち，密度行列 $\Lambda \otimes id_R(|\Phi\rangle\langle\Phi|)$ の固有値と密度行列 $\Lambda_E(\rho)$ の固有値は一致する．したがって，$H(\Lambda \otimes id_R(|\Phi\rangle\langle\Phi|)) = H(\Lambda_E(\rho))$ となり，$I_c(\rho,\Lambda) = H(\Lambda(\rho)) - H(\Lambda_E(\rho))$ を得る．

演習問題 5　(2.41) を示せ．

2.5 Qubit 系

次に，量子系の最も典型例である $\mathbb{C}^2$ の場合を考えよう．この場合は，bit の量子版として，qubit とよばれる．qubit 系での密度行列は 3 つの行列

$$E^1 := \frac{1}{2}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E^2 := \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad E^3 := \frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.43}$$

と 3 次元ベクトル $\boldsymbol{x} \in \mathbb{R}^3$ を用いて定義される状態表記 $\rho_{\boldsymbol{x}} := \frac{1}{2}I + \sum_{j=1}^{3} x_j E^j$ を得る．$\rho_{\boldsymbol{x}}$ が密度行列になるための必要十分条件は $\|\boldsymbol{x}\| \le 1$ であり，純粋状態となるための必要十分条件は $\|\boldsymbol{x}\| = 1$ である．また，任意の系 $\mathbb{C}^2$ 上の密度行列は上記の形で表すことができる．この表示の下で，密度行列 $\rho_{\boldsymbol{x}}$ の固有値は $\frac{1+\|\boldsymbol{x}\|}{2}, \frac{1-\|\boldsymbol{x}\|}{2}$ となる．したがって，$H(\rho_{\boldsymbol{x}}) = h(\frac{1+\|\boldsymbol{x}\|}{2})$ となる．ここで，関数 $h(x)$ は **2 値エントロピー**とよばれ，$h(x) := -x\log(x) - (1-x)\log(1-x)$ で与えられる．2.4 節で与えた 2 つの状態間の相違の度合いを表す関数は，以下のように計算できる．

$$\begin{aligned}
F(\rho_{\boldsymbol{x}}, \rho_{\boldsymbol{x}'})^2 &= \frac{1 + \boldsymbol{x}\cdot\boldsymbol{x}' + \sqrt{1-\|\boldsymbol{x}\|^2}\sqrt{1-\|\boldsymbol{x}'\|^2}}{2} \qquad (2.44)\\
D(\rho_{\boldsymbol{x}}\|\rho_{\boldsymbol{x}'}) &= h\left(\frac{1+\|\boldsymbol{x}\|}{2}\right) - \frac{1+\boldsymbol{x}\cdot\boldsymbol{x}'/\|\boldsymbol{x}'\|}{2}\log\left(\frac{1+\|\boldsymbol{x}'\|}{2}\right) \\
&\quad - \frac{1-\boldsymbol{x}\cdot\boldsymbol{x}'/\|\boldsymbol{x}'\|}{2}\log\left(\frac{1-\|\boldsymbol{x}'\|}{2}\right) \\
d_1(\rho_{\boldsymbol{x}}, \rho_{\boldsymbol{x}'}) &= \frac{\|\boldsymbol{x}-\boldsymbol{x}'\|}{2} \\
e^{\psi(s|\rho_{\boldsymbol{x}}\|\rho_{\boldsymbol{x}'})} &= \frac{1+\boldsymbol{x}\cdot\boldsymbol{x}'/(\|\boldsymbol{x}\|\cdot\|\boldsymbol{x}'\|)}{2}\left(\frac{1+\|\boldsymbol{x}\|}{2}\right)^{1-s}\left(\frac{1+\|\boldsymbol{x}'\|}{2}\right)^{s} \\
&\quad + \frac{1-\boldsymbol{x}\cdot\boldsymbol{x}'/(\|\boldsymbol{x}\|\cdot\|\boldsymbol{x}'\|)}{2}\left(\frac{1-\|\boldsymbol{x}\|}{2}\right)^{1-s}\left(\frac{1+\|\boldsymbol{x}'\|}{2}\right)^{s} \\
&\quad + \frac{1-\boldsymbol{x}\cdot\boldsymbol{x}'/(\|\boldsymbol{x}\|\cdot\|\boldsymbol{x}'\|)}{2}\left(\frac{1+\|\boldsymbol{x}\|}{2}\right)^{1-s}\left(\frac{1-\|\boldsymbol{x}'\|}{2}\right)^{s} \\
&\quad + \frac{1+\boldsymbol{x}\cdot\boldsymbol{x}'/(\|\boldsymbol{x}\|\cdot\|\boldsymbol{x}'\|)}{2}\left(\frac{1-\|\boldsymbol{x}\|}{2}\right)^{1-s}\left(\frac{1-\|\boldsymbol{x}'\|}{2}\right)^{s}
\end{aligned}$$

$$D_{\max}(\rho_{\boldsymbol{x}}\|\rho_{\boldsymbol{x}'}) = \log \frac{(1-\boldsymbol{x}\cdot\boldsymbol{x}')^2 + \sqrt{\|\boldsymbol{x}-\boldsymbol{x}'\|^2 + \|\boldsymbol{x}\times\boldsymbol{x}'\|^2}}{1-\|\boldsymbol{x}'\|}$$

$$D_{\min}(\rho_{\boldsymbol{x}}\|\rho_{\boldsymbol{x}'}) = \begin{cases} -\log \frac{1+\boldsymbol{x}\cdot\boldsymbol{x}'}{2} & \|\boldsymbol{x}\| = 1 \text{ のとき} \\ 0 & \|\boldsymbol{x}\| \neq 1 \text{ のとき.} \end{cases}$$

ここで，$\boldsymbol{x}\times\boldsymbol{x}'$ は $\boldsymbol{x}$ と $\boldsymbol{x}'$ の外積を表す．2 つの純粋状態 $|y\rangle$, $|z\rangle$ の場合，$\mathbb{C}^2$ 上の 2 つの密度行列に帰着できる．すなわち，$\|\boldsymbol{x}\| = \|\boldsymbol{x}'\| = 1$, $|\langle y|z\rangle|^2 = \frac{1+\boldsymbol{x}\cdot\boldsymbol{x}'}{2}$ となる．したがって，$s \in (0,1)$ について，$e^{\psi(s\||y\rangle\langle y|\||z\rangle\langle z|)} = |\langle y|z\rangle|^2$, $d_1(|y\rangle\langle y|, |z\rangle\langle z|) = \sqrt{1-|\langle y|z\rangle|^2}$, および, $D_{\min}(|y\rangle\langle y|, |z\rangle\langle z|) = -\log|\langle z|y\rangle|^2$ を得る．一方，$|y\rangle\langle y| \neq |z\rangle\langle z|$ とすると，$s < 0$ のときの相対 Rényi エントロピー，相対エントロピー，相対 max-エントロピーは発散する．

2.6　情報処理不等式

本節では量子通信路と 2.4 節で与えた情報量との関係を述べる．2.4 節では，系 $\mathcal{H}$ 上の 2 つの密度行列 ρ_1, ρ_2 がどの程度離れているか測る関数 $f(\rho_1, \rho_2)$ を複数紹介した．

情報処理不等式：　任意の量子通信路 Λ について以下が成り立つ．

$$f(\rho_1, \rho_2) \geq f(\Lambda(\rho_1), \Lambda(\rho_2)). \tag{2.45}$$

定理 2.6.1　トレースノルム距離 $d_1(\rho_1, \rho_2)$[36, 38], Bures の距離 $b(\rho_1, \rho_2)$[36, 38], 相対エントロピー $D(\rho_1\|\rho_2)$[36, 38, 93]，$1 > s > -1$ のときの相対 Rényi エントロピー $D_{1-s}(\rho_1\|\rho_2)$[93]，相対 min-エントロピー $D_{\min}(\rho_1\|\rho_2)$[100], 相対 max-エントロピー $D_{\max}(\rho_1\|\rho_2)$[100], 対数逆平方忠実度 $F_{\log}(\rho_1, \rho_2)$[36, 38] は上記の情報処理不等式を満たす．

一方，$\tilde{F}(\rho_1, \rho_2)$ は必ずしも情報処理不等式を満たさない．任意の量子通信路は Stinespring 表現を持つことから，部分トレースの場合に情報処理不等式を示せば，任意の量子通信路について (2.45) が成り立つ．

ρ_2 が完全混合状態 ρ_{mix} のとき，相対エントロピー，相対 Rényi エントロピー，相対 min-エントロピー，相対 max-エントロピーは対象となる系の次元

を d とすると，それぞれ von Neumann エントロピー，Rényi エントロピー，max-エントロピー，min-エントロピーを用いて以下のように与えられる．

$$D(\rho\|\rho_{\mathrm{mix}}) = \log d - H(\rho), \qquad D_{1-s}(\rho\|\rho_{\mathrm{mix}}) = \log d - H_{1-s}(\rho)$$

$$D_{\min}(\rho\|\rho_{\mathrm{mix}}) = \log d - H_{\max}(\rho), \qquad D_{\max}(\rho\|\rho_{\mathrm{mix}}) = \log d - H_{\min}(\rho).$$

上記の事実に定理 2.6.1 を組み合わせることで以下の系を得る．

系 2.6.2 系 $\mathcal{H}$ から系 $\mathcal{H}$ へのユニタルな量子通信路 Λ について，以下が成り立つ．

$$H(\rho) \geq H(\Lambda(\rho)), \qquad H_{1-s}(\rho) \geq H_{1-s}(\Lambda(\rho))$$

$$H_{\max}(\rho) \geq H_{\max}(\Lambda(\rho)), \qquad H_{\min}(\rho) \geq H_{\min}(\Lambda(\rho)).$$

ただし，$1 > s \geq -1$ とする．

系 $\mathcal{H}$ 上の状態 ρ_1, ρ_2, ρ_1', ρ_2' と実数 $1 > \lambda > 1$ に対して，系 $\mathcal{H} \otimes \mathbb{C}^2$ 上の状態 $\tilde{\rho_1} := \begin{pmatrix} \lambda\rho_1 & 0 \\ 0 & (1-\lambda)\rho_1' \end{pmatrix}$, $\tilde{\rho_2} := \begin{pmatrix} \lambda\rho_2 & 0 \\ 0 & (1-\lambda)\rho_2' \end{pmatrix}$ を考え，系 $\mathbb{C}^2$ についての部分トレースに定理 2.6.1 を適用する．$\tilde{\rho_1}$, $\tilde{\rho_2}$ の場合に，それぞれの情報量を計算することで以下の系を得る．

系 2.6.3 トレースノルム距離，Bures の距離の二乗，相対エントロピー，相対 min-エントロピー，$-1 < s < 0$ のときの $e^{\psi(s|\rho_1\|\rho_2)}$ は全て，接合凸性を満たす．他に，$1 > s > 0$ のとき，$-e^{\psi(s|\rho_1\|\rho_2)}$ や $-F(\rho_1, \rho_2)$ も接合凸性を満たす．

さらに，ρ_2, ρ_2' が完全混合状態 ρ_{mix} である場合に，系 2.6.3 を適用することで以下の系を得る．

系 2.6.4 von Neumann エントロピー $H(\rho)$ は凹性を満たし，$e^{\psi(s|\rho)}$ は $s < 0$ のとき凸性を満たし，$0 < s < 1$ のとき凹性を満たす．

2.7 相対エントロピーと Rényi エントロピーの関係

量子情報理論では，与えられた密度行列 ρ と実数 R から決まる最小値

$\min_{H(\rho')\le R} D(\rho'\|\rho)$ や $\min_{H(\rho')\ge R} D(\rho'\|\rho)$ が重要な意味を持つことがある．この値は状態 $\rho = \rho(\boldsymbol{p})$ の $\psi(s) := \psi(s|\boldsymbol{p}) = \psi(s|\rho)$ を用いて表すこともできる．本節では，初めに状態 $\rho = \rho(\boldsymbol{p})$ の $\psi(s)$ の微分が相対エントロピーを用いて表せることを示す．この事実を用いて，上記の値を $\psi(s)$ を用いて与える公式を示す．以下では，$\boldsymbol{p} = (p_1, \ldots, p_d)$ は $p_j \ge p_{j+1}$, $p_d > 0$ を満たす場合について扱う．

初めに，$\psi(s)$ の微分に注目する．(2.27) より，関数 $\psi'(s)$ は単調増加となる．

$$\lim_{s\to-\infty} \psi'(s) = \log p_1 = H_{\min}(\rho), \quad \psi'(1) = -\sum_{j=1}^{r} \log p_j$$

となるので，$S \in (H_{\min}(\rho), \psi'(1)]$ に対して，$\psi'(s)$ の逆関数として $s(S)$ を定めことができる．すなわち，

$$S = \psi'(s(S)) \tag{2.46}$$

を満たす $s(S) \in (-\infty, 1]$ を定める．

さらに，$p_1 = p_k > p_{k+1}$ を満たすように k を選ぶ．すると，$S \in (H_{\min}(\rho), \psi'(1)]$ に対して，

$$\begin{aligned}\frac{d}{dS}(1-s(S))S + \psi(s(S)) &= 1 - s(S) - s'(S)S + s'(S)\psi'(s(S)) \\ &= 1 - s(S) > 0\end{aligned}$$

が成り立ち，$(1-s(S))S + \psi(s(S))$ は S の関数として単調増加となる．そして，$(1-1)\psi'(1) + \psi(1) = \psi(1) = \log d$ が成り立ち，後に示すように，

$$\lim_{s\to-\infty} (1-s)\psi'(s) + \psi(s) = \log k \tag{2.47}$$

が成り立つ．したがって，$R \in (\log k, \log d]$ に対して，逆関数 S_R を以下で定義する．

$$R = (1 - s(S_R))S_R + \psi(s(S_R)). \tag{2.48}$$

逆に，$R \le \log k$ となる R は任意の s について

$$R < -s\psi'(s) + \psi(s) \tag{2.49}$$

を満たす.

(2.47) の証明.

$$
\begin{aligned}
\psi'(s)(1-s)+\psi(s) &= -(1-s)\sum_{j=1}^{d}\frac{p_j^{1-s}\log p_j}{\sum_{j'=1}^{d}a_{j'}^{1-s}}+\log\sum_{j'=1}^{d}p_{j'}^{1-s}\\
&= -(1-s)\sum_{j=k+1}^{d}\frac{p_j^{1-s}\log p_j}{\sum_{j'=1}^{d}p_{j'}^{1-s}}+\log\sum_{j'=1}^{d}p_{j'}^{1-s}-\log kp_1^{1-s}\\
&\quad+\left(-k(1-s)\frac{p_1^{1-s}\log p_1}{\sum_{j'=1}^{d}p_{j'}^{1-s}}+(1-s)\log p_1\right)+\log k\\
&= -(1-s)\sum_{j=k+1}^{d}\frac{p_j^{1-s}\log p_j}{\sum_{j'=1}^{d}p_{j'}^{1-s}}+\log\frac{\sum_{j'=1}^{d}p_{j'}^{1-s}}{kp_1^{1-s}}\\
&\quad+(1-s)\frac{\sum_{j=k+1}^{d}p_j^{1-s}}{\sum_{j'=1}^{d}p_{j'}^{1-s}}\log p_1+\log k.
\end{aligned}
$$

$j>k$ について, $\frac{p_j^{1-s}}{\sum_{j'=1}^{d}p_{j'}^{1-s}}$ は $s\to-\infty$ の極限において 0 に指数的に収束する. 一方, $\frac{\sum_{j=1}^{d}p_j^{1-s}}{kp_1^{1-s}}$ は 1 に収束する. したがって, (2.47) を得る. □

上で定義した関数 $s(S)$ と S_R を用いると, 以下の補題のように最小値 $\min_{H(\rho')=R}D(\rho'\|\rho)$ を特徴付けることができる.

補題 2.7.1 $R\in(\log k,\log d]$ に対して,

$$
S_R-R=S_R s(S_R)-\psi(s(S_R))=\frac{s(S_R)R-\psi(s(S_R))}{1-s(S_R)} \tag{2.50}
$$

$$
=\min_{H(\boldsymbol{q})=R}D(\boldsymbol{p}\|\boldsymbol{p})=\min_{H(\rho')=R}D(\rho'\|\rho) \tag{2.51}
$$

が成り立つ. そして, $R\in[0,\log k]$ に対して,

$$
\min_{H(\boldsymbol{q})=R}D(\boldsymbol{q}\|\boldsymbol{p})=\min_{H(\rho')=R}D(\rho'\|\rho)=-\log p_1-R \tag{2.52}
$$

が成り立つ.

証明.　最初の式 (2.50) の第1式は (2.48) から直ちに得られる．(2.48) より，$S_R = \frac{R-\psi(s(S_R))}{1-s(S_R)}$ が得られる．この式を $S_R - R$ に代入することで (2.50) の第2式を示すことができる．

以下では (2.51) を示す．$\rho_s := \frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}$ とすると，

$$
\begin{aligned}
&D(\rho'\|\rho) - D(\rho_s\|\rho)\\
=&\operatorname{Tr}\rho'(\log\rho' - \log\rho) - \operatorname{Tr}\frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\left(\log\frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}} - \log\rho\right)\\
=&\operatorname{Tr}\rho'\left(\log\rho' - \log\frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\right) + \operatorname{Tr}\left(\rho' - \frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\right)\left(\log\frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}} - \log\rho\right)\\
=&D(\rho'\|\rho_s) - s\operatorname{Tr}\left(\rho' - \frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\right)\log\rho \qquad (2.53)
\end{aligned}
$$

および，

$$
\begin{aligned}
&-H(\rho') + H(\rho_s)\\
&\quad= \operatorname{Tr}\rho'\left(\log\rho' - \log\frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\right) + \operatorname{Tr}\left(\rho' - \frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\right)\log\frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\\
&\quad= D(\rho'\|\rho_s) + (1-s)\operatorname{Tr}\left(\rho' - \frac{\rho^{1-s}}{\operatorname{Tr}\rho^{1-s}}\right)\log\rho \qquad (2.54)
\end{aligned}
$$

が成り立つ．

さらに，(2.48) から $H(\rho_{s(S_R)}) = R$ を得る．$H(\rho') = R$ とすると，(2.53), (2.54) より，

$$
\frac{D(\rho'\|\rho_{s(S_R)})}{1-s(S_R)} = -\operatorname{Tr}\left(\rho' - \rho_{s(S_R)}\right)\log\rho = \frac{D(\rho'\|\rho) - D(\rho_{s(S_R)}\|\rho) - D(\rho'\|\rho_{s(S_R)})}{s(S_R)}
$$

となる．すなわち，

$$
D(\rho'\|\rho) - D(\rho_{s(S_R)}\|\rho) = \frac{1}{1-s(S_R)}D(\rho'\|\rho_{s(S_R)}) \geq 0.
$$

したがって，$D(\rho_{s(S_R)}\|\rho) = \min_{H(\rho')=R} D(\rho'\|\rho)$ を得る．また，ρ_s は適切に $\boldsymbol{q}$ を選ぶと，$\rho(\boldsymbol{q})$ と書ける．したがって，$\boldsymbol{q}$ を $\rho(\boldsymbol{q})$ と同一視することで，上

記の値が $\min_{H(\boldsymbol{q})=R} D(\boldsymbol{q}\|\boldsymbol{p})$ とも等しいことが確認できる．さらに，(2.48) より，

$$D(\rho_{s(S_R)}\|\rho) = \psi'(s(S_R))s(S_R) - \psi(s(S_R)) = S_R s(S_R) - \psi(s(S_R))$$

となるので，(2.51) を得る．

次に (2.52) を示す．$R \in [0, \log k]$ について，ρ' を $H(\rho') = R$ を満たすように選ぶ．すると，

$$\begin{aligned} D(\rho'\|\rho) &= \operatorname{Tr} \rho' \log \rho' + \operatorname{Tr} \rho'(-\log \rho) \\ &\geq -H(\rho') + \operatorname{Tr} \rho'(-\log p_1) = -\log p_1 - R \end{aligned}$$

が成り立つ．ρ' のサポートが $|1\rangle, \ldots, |k\rangle$ で生成される部分空間になるもので，$H(\rho') = R$ となるものが存在する．そのような ρ' については上記の不等式で等号を達成する．したがって，(2.52) を得る． □

補題 2.7.1 を用いると，$\min_{H(\rho')\leq R} D(\rho'\|\rho)$ や $\min_{H(\rho')\geq R} D(\rho'\|\rho)$ に関する以下の補題を示すことができる．

補題 2.7.2 $H(\rho) < R < \log d$ のとき，

$$S_R - R = \min_{H(\boldsymbol{q})\geq R} D(\boldsymbol{q}\|\boldsymbol{p}) = \min_{H(\rho')\geq R} D(\rho'\|\rho) \tag{2.55}$$

$$0 = \min_{H(\boldsymbol{q})\leq R} D(\boldsymbol{q}\|\boldsymbol{p}) = \min_{H(\rho')\leq R} D(\rho'\|\rho) \tag{2.56}$$

が成り立つ．$\log k < R < H(\rho)$ のとき，

$$0 = \min_{H(\boldsymbol{q})\geq R} D(\boldsymbol{q}\|\boldsymbol{p}) = \min_{H(\rho')\geq R} D(\rho'\|\rho) \tag{2.57}$$

$$S_R - R = \min_{H(\boldsymbol{q})\leq R} D(\boldsymbol{q}\|\boldsymbol{p}) = \min_{H(\rho')\leq R} D(\rho'\|\rho) \tag{2.58}$$

が成り立つ．$0 \leq R \leq \log k$ のとき，

$$0 = \min_{H(\boldsymbol{q})\geq R} D(\boldsymbol{q}\|\boldsymbol{p}) = \min_{H(\rho')\geq R} D(\rho'\|\rho) \tag{2.59}$$

$$\log p_1 - R = \min_{H(\boldsymbol{q})\leq R} D(\boldsymbol{q}\|\boldsymbol{p}) = \min_{H(\rho')\leq R} D(\rho'\|\rho) \tag{2.60}$$

が成り立つ．

証明.　(2.46) の両辺を R で微分することで，

$$\frac{dS_R}{dR} = \frac{ds(S_R)}{dR}\psi''(s(S_R)) \tag{2.61}$$

を得る．次に，(2.48) の両辺を R で微分すると，$1 = -\frac{ds(S_R)}{dR}S_R + (1 - s(S_R))\frac{dS_R}{dR}s'(S_R)\psi'(s(S_R))$ となり，(2.46) を代入すると，

$$1 = (1 - s(S_R))\frac{dS_R}{dR} \tag{2.62}$$

を得る．(2.61) と (2.62) を組み合わせると，

$$\frac{ds(S_R)}{dR} = \frac{1}{(1 - s(S_R))\psi''(s(S_R))} < 0 \tag{2.63}$$

を得る．

そして，(2.62) と (2.63) より，

$$\frac{d}{dR}(S_R - R) = \frac{1}{1 - s(S_R)} - 1 = \frac{s(S_R)}{1 - s(S_R)}$$

$$\frac{d^2}{dR^2}(S_R - R) = \frac{1}{(1 - s(S_R))^3}\psi''(s(S_R)) > 0$$

を得る．したがって，関数 $R \mapsto S_R - R$ は凸関数となり，$\frac{d}{dR}(S_R - R) = 0$ となるのは，$s(S_R) = 0$，すなわち，$R = H(\rho)$ となる場合に限られる．$S_{H(\rho)} - H(\rho) = 0$ であるから，この関数は $R = H(\rho)$ のときに最小値 0 をとる．したがって，(2.51) に注意すると，(2.55), (2.56), (2.57), (2.58), (2.59) を得る．また，$\log p_1 - R$ に同様の議論を適用すると (2.60) を得る．　□

関数 ψ に関して以下の補題を得る．

補題 2.7.3　$H(\rho) < R < \log d$ のとき，

$$S_R - R = \max_{0\le s<1}\frac{sR - \psi(s)}{1-s}, \quad 0 = \max_{s\le 0}\frac{sR - \psi(s)}{1-s} \tag{2.64}$$

が成り立つ．$\log k < R < H(\rho)$ のとき，

$$0 = \max_{0\le s<1}\frac{sR - \psi(s)}{1-s}, \quad S_R - R = \max_{s\le 0}\frac{sR - \psi(s)}{1-s} \tag{2.65}$$

が成り立つ．$0 \le R \le \log k$ のとき，

$$0 = \max_{0 \le s < 1} \frac{sR - \psi(s)}{1-s}, \quad \log p_1 - R = \sup_{s \le 1} \frac{sR - \psi(s)}{1-s} \tag{2.66}$$

が成り立つ．

証明. s について微分すると以下を得る．

$$\frac{d}{ds}\frac{sR - \psi(s)}{1-s} = \frac{R - (1-s)\psi'(s) - \psi(s)}{(1-s)^2} \tag{2.67}$$

$$\frac{d}{ds}(R - (1-s)\psi'(s) - \psi(s)) = -(1-s)\psi''(s) \le 0. \tag{2.68}$$

(2.68) についての等号は $s = 1$ のときにのみ成り立つ．

$R \in (\log k, \log d)$ のとき，(2.46) と (2.48) より，

$$R - (1 - s(S_R))\psi'(s(S_R)) - \psi(s(S_R)) = 0 \tag{2.69}$$

を得る．したがって，$\max_{s<1} \frac{sR-\psi(s)}{1-s} = \frac{s(S_R)R+\psi(s(S_R))}{1-s(S_R)}$ が成り立つ．特に，補題 2.7.2 の証明で現れた (2.63) は関数 $R \mapsto s(S_R)$ が狭義単調増加であることを示している．そのため，$s(S_R) \le 0$ であることと $R \le H(\rho)$ は同値となる．したがって，$\frac{0R-\psi(0)}{1} = 0$ となることに注意すると以下を得る．

$$\max_{0 \le s < 1} \frac{sR - \psi(s)}{1-s} = \begin{cases} \frac{s(S_R)R+\psi(s(S_R))}{1-s(S_R)} & \text{if } H(\rho) < R < \log d \\ 0 & \text{if } \log k < R \le H(\rho) \end{cases}$$

$$\max_{s \le 0} \frac{sR - \psi(s)}{1-s} = \begin{cases} 0 & \text{if } H(\rho) < R < \log d \\ \frac{s(S_R)R+\psi(s(S_R))}{1-s(S_R)} & \text{if } \log k < R \le H(\rho). \end{cases}$$

よって，(2.64) の 2 つの式と (2.65) の 2 つの式を得る．

$R \in [0, \log k]$ のとき，(2.49) より，$s < 1$ について (2.67) の右辺は負の数となる．よって，

$$\sup_{s<1} \frac{sR - \psi(s)}{1-s} = \lim_{s \to -\infty} \frac{sR - \psi(s)}{1-s} = -\log p_1 - R$$

となる．ゆえに，

$$\max_{0\le s<1}\frac{sR-\psi(s)}{1-s}=0,\quad \sup_{s\le 0}\frac{sR-\psi(s)}{1-s}=-\log p_1-R$$

となり，(2.66) の 2 つの式を得る． □

以上の補題をまとめると以下の定理を得る．

定理 2.7.4

$$\begin{aligned}\min_{\boldsymbol{q}:H(\boldsymbol{q})\le R}D(\boldsymbol{q}\|\boldsymbol{p}) &= \min_{H(\rho')\le R}D(\rho'\|\rho)\\ &=\sup_{s\le 0}\frac{sR-\psi(s)}{1-s}=\sup_{s\le 0}\frac{s}{1-s}(R-H_{1-s}(\rho)),\end{aligned}\tag{2.70}$$

$$\begin{aligned}\min_{\boldsymbol{q}:H(\boldsymbol{q})\ge R}D(\boldsymbol{q}\|\boldsymbol{p}) &= \min_{H(\rho')\ge R}D(\rho'\|\rho)\\ &=\max_{0\le s<1}\frac{sR-\psi(s)}{1-s}=\max_{0\le s<1}\frac{s}{1-s}(R-H_{1-s}(\rho)).\end{aligned}\tag{2.71}$$

第3章 エンタングルメントとその定量化

3.1 局所操作

合成系 $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ の各成分となる系が遠隔地にあるとき，系全体に跨る任意の操作を行うことは一般には困難であることが多い．同じように，系全体に跨る任意の状態を生成することも同様に困難であることが多い．一方，それぞれの系での量子操作と系の間でも古典通信からなる操作は，遠隔地に跨る操作を必要としないため，そのような困難さはない．そのため，LOCC はエンタングルを増やさない．以下では，そのような操作を局所操作 (Local Operation) と古典通信 (Classical Communication) という意味で **LOCC** と記述することにする．一方，最大エンタングル状態は，遠隔地に跨った状態であるため，その実現は困難であるが，2 者間に跨った状態の中でも最も基本となる状態である．例えば，3.2 節で述べるように，2 者間の量子状態の伝送という遠隔地に跨る操作は，最大エンタングル状態と LOCC の組み合わせで実現できる．また，3.6 節で述べるように，2 者間の一般のエンタングル状態は最大エンタングル状態と LOCC の組み合わせで実現できる．このように，最大エンタングル状態に加え，LOCC はエンタングル状態を理解する上で基本となる概念である．

LOCC の中で，個別に系を 1 つずつ測定し，測定値の伝送を 1 方向に限ったものを **1 方向 LOCC** とよぶ．具体的には，以下のように書ける．系 $\mathcal{H}_1$ で

Instrument $\{\Lambda^1_{\omega_1}\}$ で与えられる測定を行い，その測定値 ω_1 を他の全ての系に送る．系 $\mathcal{H}_2$ では送られてきた測定値 ω_1 に基づいた Instrument $\{\Lambda^{2,\omega_1}_{\omega_2}\}$ で与えられる測定を行い，その測定値 ω_2 を残りの系に送る．系 $\mathcal{H}_j$ では，送られてきた測定値 $\omega_1,\ldots,\omega_{j-1}$ に基づいた Instrument $\{\Lambda^{j,\omega_1,\ldots,\omega_{j-1}}_{\omega_j}\}$ で与えられる測定を行い，その測定値 ω_j を残りの系に送る．この LOCC は以下のトレースを保存する完全正写像で与えられる．

$$\sum_{\omega_1,\omega_2,\ldots,\omega_n} \Lambda^1_{\omega_1}\otimes\Lambda^{2,\omega_1}_{\omega_2}\otimes\cdots\otimes\Lambda^{n,\omega_1,\ldots,\omega_{n-1}}_{\omega_n}. \tag{3.1}$$

一方，LOCC の中で，個別に系を複数回測定することを許し，双方向の測定値の伝送を許す状態操作を**2方向 LOCC** とよぶ．例えば，系が2つあるとき，それぞれの系で交互に測定を行い，測定値を送りあいながら状態変化をさせる方法も2方向 LOCC に含まれる．一般に，LOCC というときは2方向 LOCC を指すとする．

さらに，LOCC を含む状態変化として，セパラブルな量子通信路が挙げられる．合成系 $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_n$ から合成系 $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_n$ への量子通信路 Λ が以下の Kraus 表現を持つとき，Λ は**セパラブル**とよばれる．

$$\Lambda(\rho)=\sum_m F^1_m\otimes F^2_m\otimes\cdots\otimes F^n_m\rho(F^1_m\otimes F^2_m\otimes\cdots\otimes F^n_m)^\dagger. \tag{3.2}$$

1方向 LOCC は2方向 LOCC に含まれ，2方向 LOCC はセパラブルな量子通信路に含まれる．

このように量子系のテンソル積の構造に基づいて制限されたクラスに含まれる量子通信路を**局所操作**とよぶ．なお，1方向 LOCC，2方向 LOCC，セパラブルな操作のそれぞれによって実現できる POVM をそれぞれ，**1方向 LOCC POVM**，**2方向 LOCC POVM**，**セパラブル POVM** とよぶ．特に，POVM $M=\{M_j\}_j$ がセパラブル POVM になることとその要素 M_j が以下のように書けることは同値である．

$$M_j=\sum_l M^{1,l}_j\otimes\cdots\otimes M^{r,l}_k. \tag{3.3}$$

ただし，$M^{m,l}_j$ は系 $\mathcal{H}_m$ 上の非負定値行列である．

定理 3.1.1 (Nielsen[92]) $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の2つの純粋状態 $|\Phi\rangle$, $|\Psi\rangle$ に対して，$\rho_1 := \mathrm{Tr}_B |\Phi\rangle\langle\Phi|$, $\rho_2 := \mathrm{Tr}_B |\Psi\rangle\langle\Psi|$ とすると，$|\Phi\rangle$ を $|\Psi\rangle$ に変換する2方向 LOCC 操作が存在するための必要十分条件は $\rho_2 \succ \rho_1$ である．

3.2 量子テレポーテーション

有限次元の量子系 $\mathcal{H}_A$ 上に群 G の既約な射影的ユニタリ表現 f と $\mathcal{H}_A$ の次元 d と同じ次元の2つの系 $\mathcal{H}_B$（送信者が所有），$\mathcal{H}_C$（受信者が所有）に跨る最大エンタングル状態 $\frac{1}{\sqrt{d}}|I\rangle\rangle_{B,C}$ が与えられたとき，古典的な情報を送るだけで，量子状態を伝送することが可能となる．このようなプロトコルは**量子テレポーテーション**とよばれ，以下で与えられる．

系 $\mathcal{H}_A$ 上に送信したい状態 $|x\rangle = \sum_j x_j |j\rangle$ を準備し，送信者は系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の測定 $d\int_G |\mathsf{f}(g)\rangle\rangle_{A,B\ A,B}\langle\langle \mathsf{f}(g)|\mu_G(dg)$ を行う．そして，送信者は測定値 g を受信者に送る．最後に，受信者は g を下に，ユニタリ $\mathsf{f}(g)$ を施す．すると，

$$
\begin{aligned}
{}_{A,B}\langle\langle \mathsf{f}(g)||x\rangle_A \frac{1}{\sqrt{d}}|I\rangle\rangle_{B,C} &= \frac{1}{\sqrt{d}} \sum_{j,k,l} \overline{\mathsf{f}(g)_{j,k}} x_j \delta_{k,l} |l\rangle_C \\
&= \frac{1}{\sqrt{d}} \sum_{l} (\overline{\mathsf{f}(g)}^T x)_l |l\rangle_C .
\end{aligned}
$$

したがって，受信者の系 $\mathcal{H}_C$ の終状態は $\mathsf{f}(g)\sum_l (\overline{\mathsf{f}(g)}^T x)_l |l\rangle_C = \sum_l x_l |l\rangle_C$ となる．このように，古典情報 g の伝送だけで，（すなわち，LOCC のみで）量子状態 $|x\rangle$ の伝送に成功したことになる．一般的に最も使われるのが，既約な射影的ユニタリ表現 f が離散 Heisenberg 表現の場合である．この場合，伝送に必要な古典情報のサイズは空間 $\mathcal{H}_A$ の次元 d の二乗となる．既約な射影的ユニタリ表現 f の表現空間の次元の二乗は群 G の位数 $|G|$ よりも小さい（詳しくは [37] の (2.42) を参照）ので，離散 Heisenberg 表現の場合が伝送する古典情報のサイズが最も小さい．

遠隔地にいる3者，Alice, Bob, Charlie が存在し，Alice と Bob は互いにエンタングルした量子系 $\mathcal{H}_A$, $\mathcal{H}_B$ を持っているとする．また，Bob と Charlie も互いにエンタングルした量子系 $\mathcal{H}_{B'}$, $\mathcal{H}_C$ を持っているとする．このとき，Alice と Charlie の間には，エンタングルした量子系がない．しかし，量子テ

レポーテーションを利用すると，量子通信なしに，(すなわち，LOCC のみで) Alice と Charlie の間にエンタングルした量子系を作ることが可能となる．具体的には，Bob が $\mathcal{H}_B \otimes \mathcal{H}_{B'}$ に上記の測定を行い，その測定値を Alice に送り，Alice は測定値に応じて，$\mathcal{H}_A$ にユニタリ変換を行う．この操作を行うことで，合成系 $\mathcal{H}_A \otimes \mathcal{H}_C$ の状態は最大エンタングル状態になる．このプロトコルは**エンタングルメントスワッピング**とよばれる．

3.3　エンタングル状態の例

2 つの系の合成系（**2 体系**）$\mathcal{H}_1 \otimes \mathcal{H}_2$ 上の純粋状態は 1.2 節で述べたように，行列 X で記述でき，そのようなものは $|X\rangle\rangle$ と表される．一般にエンタングルの度合いは個別の系のユニタリ変換（**局所ユニタリ**とよぶ）によって変化しないと考えられる．したがって，エンタングルメント理論では局所ユニタリで移りあうエンタングル状態は同値として扱う．そのため，(1.8) で与えた X の Schmidt 係数によってエンタングルメントは特徴付けられる．特に，Schmidt ランクが d であり，Schmidt 係数が一定値である場合，その純粋状態 $|X\rangle\rangle$ はランク d の最大エンタングルとなる．$\mathcal{H}_1$ と $\mathcal{H}_2$ の次元がともに d の場合，純粋状態 $|X\rangle\rangle$ がランク d の最大エンタングルとなることと，$\sqrt{d}X$ がユニタリ行列となることが同値である．

一方，混合状態の場合はその特徴付けは簡単ではない．$\mathcal{H}_1 = \mathcal{H}_2$ 上の $\mathbb{X}^{2r}$ の離散 Heisenberg 表現 $\mathsf{W}^r_{\mathbb{X}}$ が与えられたとき，$\mathbb{X}^{2r}$ 上の確率分布 P を用いて，混合状態 $\sum_{\vec{s} \in \mathbb{X}^{2r}} \mathrm{P}(\vec{s})|\mathsf{W}^r_{\mathbb{X}}(\vec{s})\rangle\rangle\langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s})|$ を **Bell 対角状態**とよぶ．このような状態は，他の一般の混合状態に比べて扱いが容易となる．

しかし，3 つ以上の系の合成系（**多体系**）$\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_r$ 上の状態のエンタングル状態の扱いは容易ではない．多体系の純粋状態として，最もよく扱われるのは，Stabilizer 状態である．それぞれの系 $\mathcal{H}_j$ の次元が $q = p^n$ であり，その合成系 $(\mathbb{C}^q)^{\otimes r} := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_r$ 上に $\mathbb{F}_q^{2r}$ の離散 Heisenberg 表現 $\mathsf{W}^r_{\mathbb{F}_q}$ が与えられた場合を考える．この設定では，[37] の 7.3.2 項で与えられるメタプレクティク表現 $\mathsf{S}^r_{\mathbb{F}_q}$ の下での離散シンプレクティク群 $\mathrm{Sp}(2r, \mathbb{F}_q)^r$ の部分群 $\mathrm{Sp}(2, \mathbb{F}_q)^r$ の作用や離散 Heisenberg 表現 $\mathsf{W}^r_{\mathbb{F}_q}$ の下での $\mathbb{F}_q^{2r}$ の作用は局所ユニタリとなる．$\mathbb{F}_q^{2r}$ の狭義自己直交部分群 N を考える．任意の要素 $\vec{s}, \vec{s}' \in N$ に対して，$\mathsf{W}^r_{\mathbb{F}_q}(\vec{s})$, $\mathsf{W}^r_{\mathbb{F}_q}(\vec{s}')$ は互いに可換である．したがって，同時固有ベ

クトルが存在する．すなわち，$x \in N^*$ に対して，以下を満たすベクトル $|v_x\rangle \in (\mathbb{C}^q)^{\otimes r}$ が存在する．

$$\mathsf{W}^r_{\mathbb{F}_q}(\vec{s})|v^N_x\rangle = \omega_{\mathbb{F}}^{x(\vec{s})}|v^N_x\rangle, \quad \forall \vec{s} \in N. \tag{3.4}$$

このような純粋状態を N の **Stabilizer 状態**とよぶ．同じ，N の Stabilizer 状態は互いに，$\mathbb{F}_q^{2r}$ の作用で移りあうので，エンタングル状態としては同値となる．また，2つの狭義自己直交部分群 N, N' に対して，シンプレクティク群 $\mathrm{Sp}(2r, \mathbb{F}_q)^r$ の部分群 $\mathrm{Sp}(2, \mathbb{F}_q)^r$ の要素 g で，$N = gN'$ となる場合，それぞれに対応する Stabilizer 状態は互いに同値となる．

実は，狭義自己直交部分群 N は $2r \times r$ の生成行列 A を用いて表すことができる．（文献 [37] の 7.2.3 項を参照のこと．）さらに，生成行列 A の上半分が可逆行列 $g \in \mathrm{GL}(r, \mathbb{F}_q)$ である場合，Ag^{-1} も同じ狭義自己直交部分群 N の生成行列となる．したがって，この条件を満たす狭義自己直交部分群 N の生成行列は，対称行列 ζ を用いて $\begin{pmatrix} I \\ \zeta \end{pmatrix}$ と表される．対称行列 ζ と $\boldsymbol{s} \in \mathbb{F}_q^r$ に対して，$\begin{pmatrix} I \\ \zeta \end{pmatrix}$ を生成行列とする狭義自己直交部分群の Stabilizer 状態で以下を満たすものを $|u^\zeta_{\boldsymbol{s}}\rangle$ とする．

$$\mathsf{W}^r_{\mathbb{F}_q}((\boldsymbol{t}, \zeta\boldsymbol{t})^T)|u^\zeta_{\boldsymbol{s}}\rangle = \omega_{\mathbb{F}}^{\boldsymbol{s}\cdot\boldsymbol{t}}|u^\zeta_{\boldsymbol{s}}\rangle, \quad \boldsymbol{t} \in \mathbb{F}_q^r. \tag{3.5}$$

このとき以下の補題が成り立つので，Stabilizer 状態を上記のタイプのものに限っても一般性を失わない．

補題 3.3.1 任意の狭義自己直交部分群 N と $x \in N^*$ に対して，$|v^N_x\rangle$ がエンタングル状態として $|u^\zeta_{\boldsymbol{s}}\rangle$ と同値となる対角成分が 0 となる対称行列 ζ と $\boldsymbol{s} \in \mathbb{F}_q^r$ が存在する．

証明. N の生成行列 A の上半分が非可逆であっても，適切な $h \in \mathrm{GL}(r, \mathbb{F}_q)$ を選ぶと，Ah の上半分は対角行列となり，その対角成分は 1 または 0 となる．Ah が狭義自己直交部分群の生成行列であることから，Ah の上半分の第 j,j 成分が 0 であるとき，Ah の下半分の第 j,j 成分 a_j は 0 でない．したがって，

$$J_{r,j} := -|j\rangle\langle j+r| + |j+r\rangle\langle j| + \sum_{k\neq j}(|k\rangle\langle k| + |k+r\rangle\langle k+r|) \tag{3.6}$$

を用いると，$J_{r,j}Ah$ の上半分の第 j,j 成分が a_j となる．この操作を繰り返すと，N と同値な狭義自己直交部分群でその生成行列 A の上半分が単位行列となるものがとれる．したがって，$|u_{\boldsymbol{s}}^{\zeta}\rangle$ が同値となる対称行列 ζ と $\boldsymbol{s}\in\mathbb{F}_q^r$ がとれる．ζ の対角成分が z_j であるとき，$\begin{pmatrix} I \\ \zeta \end{pmatrix}$ に $Q_{z_1}\oplus\cdots\oplus Q_{z_r}\in \mathrm{Sp}(2,\mathbb{F}_q)^r$ を左から掛けて得られる行列は上半分は単位行列となり，下半分は対角成分が 0 となる対称行列となる．□

以下，$\mathbb{F}_q=\mathbb{F}_2$ の場合を扱う．この場合，$r\times r$ の対称行列 ζ の成分は 0 または 1 となる．特に，対角成分が 0 となる ζ について個々の系 $\mathcal{H}_j$ を点で表し，ζ の k,j 成分が 1 となる組のみ辺で結ぶと**グラフ**が得られる．以下では，r 個の点からなるグラフと対角成分が 0 となる $r\times r$ の対称行列 ζ を同一視することができる．したがって，グラフ ζ と $\boldsymbol{s}\in\mathbb{F}_2^r$ から決まる Stabilizer 状態 $|u_{\boldsymbol{s}}^{\zeta}\rangle$ をグラフ ζ の**グラフ状態**とよぶことにする [56, 57].

グラフ ζ と点 j,k から決まる $\mathrm{Sp}(2,\mathbb{F}_2)$ の要素 $g_{j,k}$ を以下で定義する．

$$g_{j,k} := \begin{cases} Q_1 & k=j\text{ のとき} \\ P_1 & \zeta_{k,j}=1\text{ のとき} \\ I & \text{上記以外.} \end{cases} \tag{3.7}$$

そして，ユニタリ行列 K_j を以下で定義する．

$$K_j := \mathsf{S}_{\mathbb{F}_q,j}(g_j), \quad g_j := g_{j,1}\oplus\cdots\oplus g_{j,r}. \tag{3.8}$$

このとき，K_j は局所ユニタリとなる．ここで，$\mathsf{S}_{\mathbb{F}_q,k}$ は k 番目のテンソル積の成分となる空間への作用を表す．点 j に対してグラフの ζ を以下のグラフ $\hat{\zeta}$ に移す変換を点 j における **local complementation** とよぶことにする．

$$\hat{\zeta}_{k,l} := \begin{cases} \zeta_{k,l} & \zeta_{j,k}\zeta_{j,l}=0\text{ となるとき} \\ 1-\zeta_{k,l} & \zeta_{j,k}\zeta_{j,l}=1\text{ となるとき.} \end{cases} \tag{3.9}$$

補題 3.3.2 状態 $K_j|u_{\boldsymbol{s}}^{\zeta}\rangle$ は点 j における local complementation を ζ に施して得られるグラフのグラフ状態となる．すなわち，local complementation によって移りあうグラフのグラフ状態は互いに同値となる．

証明. $g_j\begin{pmatrix} I \\ \zeta \end{pmatrix}$ で生成されるベクトル空間が $\begin{pmatrix} I \\ \hat{\zeta} \end{pmatrix}$ で生成されるベクトル空間に一致することを示せば十分である．$r=3$ の場合，$g_1 = Q_1 \oplus P_1 \oplus P_1$

$$\zeta = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \hat{\zeta} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

の場合に，$\begin{pmatrix} I \\ \zeta \end{pmatrix}$ で生成されるベクトル空間と $\begin{pmatrix} I \\ \hat{\zeta} \end{pmatrix}$ で生成されるベクトル空間が g_1 の作用で互いに移りあうことが簡単な計算により確認できる．したがって，$r=3$ の場合について，上記の事実を得る．さらに，一般の場合についても $r=3$ の場合の事実を用いて示すことができる． □

グラフに対して，その j,k 成分の値を反転させる操作を $\mathcal{T}_{j,k}$ とする．このとき以下の補題が成り立つ．

補題 3.3.3 C-NOT 演算である $\sum_{\boldsymbol{x}\in\mathbb{F}_q^r}|Q_{j,l:1}\boldsymbol{x}\rangle\langle\boldsymbol{x}|$ は，グラフ ζ のグラフ状態をグラフ $\mathcal{T}_{j,l}(\zeta)$ のグラフ状態に移す．ここで，$Q_{j,l:1} = |k)(l| + \sum_{k=1}^r |k)(k|$ であり，$\{|k)\}_{k=1}^r$ は有限体 $\mathbb{F}_q$ 上のベクトル空間 $\mathbb{F}_q^r$ の基底である．（メタプレクティク表現 $\mathsf{S}_{\mathbb{F}_q}^r$ との関係においては，$\sum_{\boldsymbol{x}\in\mathbb{F}_q^r}|Q_{j,l:1}\boldsymbol{x}\rangle\langle\boldsymbol{x}|$ は [37] の 7.3.2 項で定義された $\mathsf{S}_{\mathbb{F}_q}^r(M_{Q_{j,l:1}})$ で与えられる．）

証明. $r=2$ の場合について示せば，他の場合は容易に一般化できる．$\zeta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\hat{\zeta} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ の場合に，$\begin{pmatrix} I \\ \zeta \end{pmatrix}$ で生成されるベクトル空間と $\begin{pmatrix} I \\ \hat{\zeta} \end{pmatrix}$ で生成されるベクトル空間が $M_{Q_{1,2:1}}$ の作用で互いに移りあうことから

この事実は確認できる．□

例 3.3.4 (1D Cluster 状態)　1次元の線の上に点が並び，隣接する点が辺で結ばれたグラフのグラフ状態を **1D Cluster 状態**とよぶ．

例 3.3.5 (Ring 状態)　円周上に点が並び，隣接する2つの点が辺で結ばれたグラフのグラフ状態を **Ring 状態**とよぶ．

例 3.3.6 (GHZ 状態)　全ての点が辺で結ばれているグラフは**完全グラフ**とよばれる．一方，ある1点 j と他の全ての点が辺で結ばれており，他に辺が存在しないとき，そのグラフは j を中心する**星グラフ**とよばれる．点 j での local complementation によって，完全グラフと j を中心する星グラフは互いに移りあう．特に， j を中心する星グラフのグラフ状態は **GHZ 状態**とよばれる．

例 3.3.7 (2D Cluster 状態)　碁盤の目の上に点が並び，上下，左右に隣接する点が辺で結ばれたグラフのグラフ状態を **2D Cluster 状態**とよぶ．

3.4　セパラブル状態の特徴付け

セパラブル状態が満たす数学的性質は複数知られている．量子系 $\mathcal{H}_A$ 上の状態 ρ を ρ^T に移す写像 τ_A を考える．この写像は状態を状態に移す線形な写像であるが，量子通信路にはならない．なぜなら，合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上での写像 ($\mathcal{H}_A$ についての**部分転置**) $\tau_A \otimes id_B$ は状態を状態に移さないからである．すなわち，$\tau_A \otimes id_B$ は正値性を保存しない．しかし，ρ が合成系 $\mathcal{H}_A \otimes \mathcal{H}_B$ 上でセパラブル状態であるとき，$\tau_A \otimes id_B(\rho)$ は $\tau_A \otimes id_B(\rho) \geq 0$ を満たし，状態となる．この条件は **PPT 条件**とよばれ，これを満たす状態は **PPT 状態**とよばれる．この条件を $\mathcal{H}_B$ についての部分転置に置き換えても同値である．なぜなら，$\tau_A \otimes id_B(\rho) \geq 0$ となることと，$id_A \otimes \tau_B(\rho) = (\tau_A \otimes id_B(\rho))^T \geq 0$ が同値であるからである．この条件は一見すると $\mathcal{H}_A$ での基底のとり方に依存するように見えるが，依存しない．定義より， $\mathcal{H}_B$ での基底のとり方に依存しない．また，同値な条件 $id_A \otimes \tau_B(\rho) \geq 0$ は $\mathcal{H}_A$ での基底のとり方に依存しない．したがって，PPT 条件は基底のとり方に依存しない．

次に，最大エンタングル状態の生成不可能性が挙げられる．すなわち，ρ の n 回テンソル積状態 $\rho^{\otimes n}$ が準備できたときに，どのような LOCC 操作 Λ_n の系列を準備しても，$\Lambda_n(\rho^{\otimes n})$ は $(\mathbb{C}^2)^{\otimes 2}$ 上の最大エンタングル状態に近づかない．この性質は，**蒸留不可能条件**とよばれる．他にも，いくつかのセパラブル状態が満たす条件が知られており，それらは，以下の定理としてまとめられる．

定理 3.4.1　$\mathcal{H}_A \otimes \mathcal{H}_B$ 上の状態 ρ についての以下の条件の間には，関係 **(1)**⇒ **(2)**⇒ **(3)**⇒ **(4)**⇒ **(5)** が成り立つ．

(1)　**セパラブル条件**　ρ はセパラブル状態である．

(2)　**PPT 条件**　$\tau_A \otimes id_B(\rho) \geq 0$.

(3)　**蒸留不可能条件**　LOCC 操作 Λ_n の系列で $\Lambda_n(\rho^{\otimes n})$ が $(\mathbb{C}^2)^{\otimes 2}$ 上の最大エンタングル状態に収束するものは存在しない．

(4)　**Reduction 条件**　$(\mathrm{Tr}_B\,\rho) \otimes I_B \geq \rho$ が成り立つ．

(5)　**Majorization 条件**　$(\mathrm{Tr}_B\,\rho) \succ \rho$ が成り立つ．

(1)⇒**(2)** については計算により確認できる．**(2)**⇒**(3)** は後の 3.5.3 項で示される．**(3)**⇒**(4)**, **(4)**⇒**(5)** については，それぞれ，Horodecki[66], Hiroshima[61] を参照のこと．なお，$\mathbb{C}^2 \otimes \mathbb{C}^2$, $\mathbb{C}^2 \otimes \mathbb{C}^3$ の場合には，**(1)** と **(2)** の同値性は示されている [67]．しかし，$\mathbb{C}^2 \otimes \mathbb{C}^4$, $\mathbb{C}^3 \otimes \mathbb{C}^3$ の場合には，**(2)** を満たすが **(1)** を満たさない反例が知られている [65]．そのような状態は**束縛エンタングル状態**とよばれる．

3.5　エンタングルメントの定量化 I：幾何学的方法

3.5.1　定義とエンタングル単調性

合成系 $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ 上の状態 ρ がこれらの系の間でどの程度のエンタングルメントがあるか測る 1 つの方法は，まったくエンタングルメントがない状態（セパラブル状態）から離れている度合いを用いる方法である．1 つ目の方法は，2.4 節で与えた 2 つの状態の相違の度合いを用い，どの程度セパラブル状態から離れているか測る方法である．なお，このような量は局所操作の下で増加しないことが自然である．そのような性質を**エンタングルメント単調**という．例えば，2 方向 LOCC の下で増加しない場合，LOCC エンタングルメント

単調といい，セパラブルな量子通信路の下で増加しない場合，セパラブルエンタングルメント単調という．

SEP を合成系 $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ 上のセパラブル状態の集合とし，2つの状態に対して定義される関数 f を用いて $E[f]_{1,\ldots,n}(\rho) := \min_{\rho_1 \in \mathrm{SEP}} f(\rho, \rho_1)$ で与えられる量がエンタングルメントの基準量の1つとして考えられる．特に，注目する系を明示しなくても混乱の恐れがない場合は，$E[f](\rho)$ と記す．そして，f として相対エントロピー $D(\rho\|\rho_1)$ を用いた場合の $E[f](\rho)$ は $E_R(\rho)$ と記し，**エンタングルメント相対エントロピー**とよぶ [117, 118]．他に，f として相対 Rényi エントロピー $D_{1-s}(\rho\|\rho_1)$, 対数逆平方忠実度, 対数逆擬忠実度を用いた場合の $E[f](\rho)$ は $E_{R,s}(\rho)$, $E_{G,1}(\rho)$, $E_{G,2}(\rho)$ と記す．ρ が純粋状態のとき，$E_{G,1}(\rho)$ と $E_{G,2}(\rho)$ は一致し，**Geometric measure** とよばれる [105, 114]．

このとき，以下の補題を得る．

補題 3.5.1　f が情報処理不等式を満たすとき，$E[f]$ はセパラブルエンタングルメント単調である．

したがって，$D_{1-s}(\rho\|\rho_1)$, $D(\rho\|\rho_1)$，対数逆平方忠実度は情報処理不等式を満たすため，$E_R(\rho)$, $E_{R,1-s}(\rho)$, $E_{G,1}(\rho)$ はセパラブルエンタングルメント単調である．一方，$E_{G,2}(\rho)$ はセパラブルエンタングルメント単調とは限らず，その意味は不明確である．しかし，単純化 $E_{G,2}(\rho) = -\log \max_{|a\rangle\langle a| \in \mathrm{SEP}} \langle a|\rho|a\rangle$ が可能である．そのため，他のエンタングルメントの基準量の計算において，重要な役割を果たすことがある．

証明.　Λ をセパラブルな量子通信路とする．ρ_1 が Λ の入力系のセパラブル状態のとき，$\Lambda(\rho_1)$ は Λ の出力系のセパラブル状態となる．ρ を Λ の入力系の状態とすると，情報処理不等式から，

$$\min_{\rho_1 \in \mathrm{SEP}} f(\rho, \rho_1) \geq \min_{\rho_1 \in \mathrm{SEP}} f(\Lambda(\rho), \Lambda(\rho_1)) \geq \min_{\rho_1' \in \mathrm{SEP}} f(\Lambda(\rho), \rho_1')$$

となり，題意を得る．　□

さらに以下の補題も成り立つ．

補題 3.5.2　f が接合凸性を満たすとき，$E[f](\rho)$ は凸関数である．

したがって，系 2.6.3 より，$E_R(\rho)$ は凸関数となる．

証明. $\rho = \lambda\rho_a + (1-\lambda)\rho_b$ とし，$\rho_{a,1} := \operatorname{argmin}_{\rho_1 \in \mathrm{SEP}} f(\rho_a, \rho_1)$，$\rho_{b,1} := \operatorname{argmin}_{\rho_1 \in \mathrm{SEP}} f(\rho_b, \rho_1)$ とする．

$$E[f](\rho) = \min_{\rho_1 \in \mathrm{SEP}} f(\rho, \rho_1) \le f(\lambda\rho_a + (1-\lambda)\rho_b, \lambda\rho_{a,1} + (1-\lambda)\rho_{b,1})$$

$$\le \lambda f(\rho_a, \rho_{a,1}) + (1-\lambda) f(\rho_b, \rho_{b,1}) = \lambda E[f](\rho_1) + (1-\lambda) E[f](\rho_2)$$

が成り立ち題意を得る． □

もう 1 つの幾何学的な方法として，以下に定義する**対数ロバスト度** $R_L(\rho)$ [119] と**大域的対数ロバスト度** $R_{L,g}(\rho)$ [33] がある．

$$R_{L:1,\ldots,n}(\rho) := \min\left\{ \log(1+t) \,\middle|\, \frac{\rho + t\rho'}{1+t} \in \mathrm{SEP} \text{ となる } \rho' \in \mathrm{SEP} \text{ が存在する} \right\}$$

$$R_{L,g:1,\ldots,n}(\rho) := \min\left\{ \log(1+t) \,\middle|\, \frac{\rho + t\rho'}{1+t} \in \mathrm{SEP} \text{ となる状態} \rho' \text{が存在する} \right\}.$$

これらの量についても，注目する系を明示しなくても混乱の恐れがない場合は，添え字 $:1,\ldots,n$ を省略することとする．定義より，$R_L(\rho) \ge R_{L,g}(\rho)$ が成り立つ．

これまで定義した量は全て，集合 SEP の中で状態を選ぶことで，最小化を行うことで定義している．したがって，最小化をとる範囲を広くとると，より小さい値となる．上記の定義では，n 個の系からなる合成系としてセパラブル状態を定義した．しかし，n 個の系を部分集合 $S \subset \{1,\ldots,n\}$ とその補集合 S^c の 2 つのグループに分け，2 つの系 $\bigotimes_{j \in S} \mathcal{H}_j$ と $\bigotimes_{j \in S^c} \mathcal{H}_j$ の 2 つの系からなる合成系として考えて，セパラブル状態を定義すると，前者で定義したセパラブル状態の集合より，後者で定義したセパラブル状態の集合の方が広いことがわかる．この事実を用いると以下の不等式を得る [82].

$$E[f]_{1,\ldots,n}(\rho) \ge E[f]_{S,S^c}(\rho). \tag{3.10}$$

後に述べるように，2 体系の場合でのエンタングルメント量の計算は比較的進んでいるため，この不等式は，エンタングルメント量の下限を与えるために強力な公式となる．なお，$R_L(\rho)$, $R_{L,g}(\rho)$ についての同じ公式が成り立つ．

さらに，ここで定義した量は局所的なユニタリの操作に関して不変である．そして，以下の関係が成り立つ [50].

補題 3.5.3　$1 > s_2 > 0,\ 0 > s_1 \geq -1$ について

$$R_{L,g}(\rho) \geq E_{R,s_1}(\rho) \geq E_R(\rho) \geq E_{R,s_2}(\rho) \tag{3.11}$$

$$E_R(\rho) \geq E_{G,2}(\rho) - H(\rho), \quad E_{R,1/2}(\rho) \geq E_{G,1}(\rho) \tag{3.12}$$

を得る．特に ρ が射影 P の定数倍，すなわち，$\frac{P}{\mathrm{Tr}\,P}$ のとき，

$$E_{R,s}(\rho) \geq E_{G,2}(\rho) - \log \mathrm{Tr}\,P, \quad E_{G,1}(\rho) \geq E_{G,2}(\rho) - \log \mathrm{Tr}\,P \tag{3.13}$$

を得る．

証明.　初めに (3.11) の第 1 式を示す．$\frac{\rho+t\rho'}{1+t} \in \mathrm{SEP}$ かつ $\log(1+t) = R_{L,g}(\rho)$ となるように，状態 ρ' と $t \geq 0$ を選ぶ．$x \mapsto -x^{s_1}$ の行列単調性より，$\frac{\rho+t\rho'}{1+t} \leq (\frac{\rho}{1+t})^{s_1}$ となる．したがって，

$$\mathrm{Tr}\,\rho^{1-s_1}\left(\frac{\rho+t\rho'}{1+t}\right)^{s_1} \leq \mathrm{Tr}\,\rho^{1-s_1}\left(\frac{\rho}{1+t}\right)^{s_1} = (1+t)^{-s_1}$$

となる．よって，

$$\begin{aligned} E_{R,s_1}(\rho) &\leq \frac{-1}{s_1}\log \mathrm{Tr}\,\rho^{1-s_1}\left(\frac{\rho+t\rho'}{1+t}\right)^{s_1} \leq \frac{-1}{s_1}\log\frac{1}{(1+t)^{s_1}} \\ &= \log(1+t) = R_{L,g}(\rho) \end{aligned}$$

となり (3.11) の第 1 式を得る．

次に，(3.12) の第 1 式を示す．ρ_1 を $E_R(\rho) = D(\rho\|\rho_1)$ 満たすセパラブルな状態とする．関数 $x \mapsto -\log x$ が凸関数であることから，(2.13) を適用すると，

$$\begin{aligned} E_R(\rho) &= D(\rho\|\rho_1) = \mathrm{Tr}\,\rho\log\rho - \mathrm{Tr}\,\rho\log\rho_1 \\ &\geq \mathrm{Tr}\,\rho\log\rho - \log\mathrm{Tr}\,\rho\rho_1 \geq E_{G,2}(\rho) - H(\rho) \end{aligned}$$

となり (3.12) の第 1 式を得る．

(3.11) の第 2 式，第 3 式，(3.11) の第 2 式はそれぞれ (2.30) の第 3 式，第 2 式，(2.29) より，直ちに確認できる．

次に，(3.13) の第 1 式を示す．ρ_1 をセパラブルな状態とする．関数 $x \mapsto x^s$ は凹関数であるから，

$$\left(\operatorname{Tr}\left(\frac{P}{\operatorname{Tr} P}\right)^{1-s}\rho_1^s\right)^{\frac{1}{s}} = \operatorname{Tr} P \left(\operatorname{Tr}\left(\frac{P}{\operatorname{Tr} P}\right)\rho_1^s\right)^{\frac{1}{s}} \le \operatorname{Tr} P \operatorname{Tr} \frac{P}{\operatorname{Tr} P}\rho_1$$

を得る．両辺の log を考えることにより，(3.13) の第 1 式を得る．

次に，(3.13) の第 2 式を示す．ρ_1 を separable な状態とする．エルミート行列 X, Y についての Schwarz 不等式 $(\operatorname{Tr} XY)^2 \le \operatorname{Tr} X^2 \operatorname{Tr} Y^2$ より，

$$\begin{aligned}\left(\operatorname{Tr}\left|\sqrt{\frac{P}{\operatorname{Tr} P}}\sqrt{\rho_1^s}\right|\right)^2 &= \frac{1}{\operatorname{Tr} P}\left(\operatorname{Tr}\left|P\sqrt{\rho_1}\right|\right)^2 = \frac{1}{\operatorname{Tr} P}\left(\operatorname{Tr}\sqrt{P\rho_1 P}\right)^2 \\ =&\frac{1}{\operatorname{Tr} P}\left(\operatorname{Tr} P\sqrt{P\rho_1 P}\right)^2 \le \frac{1}{\operatorname{Tr} P}\operatorname{Tr} P \operatorname{Tr} P\rho_1 P = \operatorname{Tr} P \operatorname{Tr}\frac{P}{\operatorname{Tr} P}\rho_1\end{aligned}$$

を得る．両辺の log を考えることにより，(3.13) の第 2 式を得る． □

3.5.2 具体例での計算

以下では具体例の場合に，エンタングルメント量を計算するが，そのために重要な性質を列挙し，その性質を用いて具体例で計算を行う．ρ が射影 P の定数倍，すなわち，$\frac{P}{\operatorname{Tr} P}$ のとき，コンパクト Lie 群 G の射影的ユニタリ表現 f に対する以下の条件 **GM1**，**GM4** および f とセパラブルな純粋状態 $|a\rangle$ に対する条件 **GM2**，**GM3**，**GM3′** を考える．

GM1 任意の $g \in G$ に対して，$\mathsf{f}(g)$ は各系のユニタリ行列のテンソル積で与えられる．

GM2 $\langle a|\rho|a\rangle = \max_{|a'\rangle\langle a'|\in \mathrm{SEP}}\langle a'|\rho|a'\rangle$.

GM3 $\int_G \mathsf{f}(g)|a\rangle\langle a|\mathsf{f}(g)^\dagger \mu(dg) \ge \langle a|\rho|a\rangle P$.

GM3′ 射影 P と $|a\rangle\langle a|$ の双方の値域を含み，以下を満たす空間 $\mathcal{H}'$ が存在する：表現 f を $\mathcal{H}'$ に制限したとき，表現 f について既約な $\mathcal{H}'$ の部分空間で P の値域と同値なものは他に存在しない．

GM4　射影 P の値域は表現 f の既約な1次元部分空間であり，表現 f について既約な部分空間で P の値域と同値なものは他に存在しない．

定理 3.5.4 ([51])　ρ が射影 P を用いて $\frac{P}{\mathrm{Tr}\,P}$ と表され，条件 **GM1**，**GM3** を満たすコンパクト Lie 群 G の射影的ユニタリ表現 f とセパラブルな純粋状態 $|a\rangle$ が存在するとき，

$$-\log\langle a|P|a\rangle \geq R_{L,g}(\rho) \tag{3.14}$$

が成り立つ．

証明.　条件 **GM3** より，

$$\langle a|\rho|a\rangle\,\mathrm{Tr}\,P\frac{P}{\mathrm{Tr}\,P}+(1-\langle a|\rho|a\rangle\,\mathrm{Tr}\,P)\rho' = \int_G \mathsf{f}(g)|a\rangle\langle a|\mathsf{f}(g)^\dagger\mu(dg)\in\mathrm{SEP}$$

を満たす状態 ρ' が存在する．したがって，$\frac{1}{1+t}=\langle a|\rho|a\rangle\,\mathrm{Tr}\,P$ となるように t を選ぶと，$-\log\langle a|P|a\rangle = \log(1+t)\geq R_{L,g}(\rho)$ となり，題意を得る．　□

定理 3.5.5 ([51])　ρ が射影 P を用いて $\frac{P}{\mathrm{Tr}\,P}$ と表され，条件 **GM1** から **GM3** を満たすコンパクト Lie 群 G の射影的ユニタリ表現 f とセパラブルな純粋状態 $|a\rangle$ が存在するとき，任意の $s\in(0,1)$ について

$$R_{L,g}(\rho)=E_R(\rho)=E_{R,s}(\rho)=E_{G,1}(\rho)=E_{G,2}(\rho)-\log\mathrm{Tr}\,P \tag{3.15}$$

が成り立つ．

証明.　補題3.5.3より，$E_{G,2}(\rho)-\log\mathrm{Tr}\,P\leq R_{L,g}(\rho)$ である．一方，**GM2** と定理3.5.4より，逆向きの不等式が成り立つので，題意を得る．　□

補題 3.5.6　ρ が射影 P の定数倍，すなわち，$\frac{P}{\mathrm{Tr}\,P}$ で与えられるとする．コンパクト Lie 群 G の射影的ユニタリ表現 f が条件 **GM1** を満たし，表現 f の下で，セパラブルな純粋状態 $|a\rangle$ は条件 **GM2**，**GM3′** を満たすとする．このとき，セパラブルな純粋状態 $|a\rangle$ は条件 **GM3** を満たす．

したがって，f が条件 **GM1** と **GM4** を満たすとき，**GM2** を満たす任意のセパラブルな純粋状態は条件 **GM3** を満たす．

ゆえに，上記いずれかの条件が成り立つとき (3.15) が成り立つ．

次に，複数のエンタングルした状態テンソル積状態について扱う．$\mathcal{H}_{1,1} \otimes \cdots \otimes \mathcal{H}_{n,1}$ 上の状態 ρ_1 と $\mathcal{H}_{1,2} \otimes \cdots \otimes \mathcal{H}_{n,2}$ 上の状態 ρ_2 が与えられたとき，テンソル積状態 $\rho_1 \otimes \rho_2$ について n 個の系 $\mathcal{H}_{1,1} \otimes \mathcal{H}_{1,2}, \ldots, \mathcal{H}_{n,1} \otimes \mathcal{H}_{n,2}$ の間のエンタングルについて，$E[f](\rho_1 \otimes \rho_2)$, $R_L(\rho_1 \otimes \rho_2)$, $R_{L,g}(\rho_1 \otimes \rho_2)$ を定義する．f が加法性を満たすとき，定義から $E[f](\rho_1 \otimes \rho_2) \le E[f](\rho_1) + E[f](\rho_2)$ を得る．同様に，$R_{L,g}(\rho_1 \otimes \rho_2) \le R_{L,g}(\rho_1) + R_{L,g}(\rho_2)$ が成り立つ．このとき，ρ の n テンソル積状態の 1 つあたりのエンタングルの量として，$E[f]_\infty(\rho) := \lim_{n\to\infty} \frac{E[f](\rho^{\otimes n})}{n}$ を定義する．$R_{L,\infty}(\rho)$, $R_{L,g,\infty}(\rho)$ についても同様に定義する．これらの量の計算のために以下の補題を考える．

補題 3.5.7 射影 P_1, P_2 から定まる 2 つの状態 $\rho_1 := \frac{P_1}{\mathrm{Tr}\, P_1}$, $\rho_2 := \frac{P_2}{\mathrm{Tr}\, P_2}$ が (3.15) を満たすとする．$E_{G,2}(\rho_1 \otimes \rho_2) = E_{G,2}(\rho_1) + E_{G,2}(\rho_2)$ となるとき，

$$R_{L,g}(\rho_1 \otimes \rho_2) = E_R(\rho_1 \otimes \rho_2) = E_{R,s}(\rho_1 \otimes \rho_2) = E_{G,1}(\rho_1 \otimes \rho_2)$$

$$= E_{G,2}(\rho_1) + E_{G,2}(\rho_2) - \log \mathrm{Tr}\, P_1 - \log \mathrm{Tr}\, P_2, \quad 1 > \forall s > 0$$

が成り立つ．

証明. 補題 3.5.3 より，

$$R_{L,g}(\rho_1 \otimes \rho_2) \ge E_{G,2}(\rho_1) + E_{G,2}(\rho_2) - \log \mathrm{Tr}\, P_1 - \log \mathrm{Tr}\, P_2$$

$$= R_{L,g}(\rho_1) + R_{L,g}(\rho_2) \ge R_{L,g}(\rho_1 \otimes \rho_2)$$

となり，$R_{L,g}(\rho_1 \otimes \rho_2) = E_{G,2}(\rho_1) + E_{G,2}(\rho_2) - \log \mathrm{Tr}\, P_1 - \log \mathrm{Tr}\, P_2$ を得る．他の値についても，同様に示せる． □

補題 3.5.8 射影 P_j $(j = 1, \ldots n)$ から定まる状態 $\rho_j := \frac{P_j}{\mathrm{Tr}\, P_j}$ に対して，条件 **GM1**，**GM4** を満たす群 $G_1, \ldots, G_n$ の射影的ユニタリ表現 $\mathsf{f}_1, \ldots, \mathsf{f}_n$ が存在するとする．このとき，$1 > s > 0$ について

$$R_{L,g}\left(\bigotimes_{j=1}^n \rho_j\right) = E_R\left(\bigotimes_{j=1}^n \rho_j\right) = E_{R,s}\left(\bigotimes_{j=1}^n \rho_j\right) = E_{G,1}\left(\bigotimes_{j=1}^n \rho_j\right)$$

$$= E_{G,2}\left(\bigotimes_{j=1}^n \rho_j\right) - \sum_{j=1}^n \log \mathrm{Tr}\, P_j$$

が成り立つ.

証明.　直積群 $G_1 \times \cdots \times G_n$ の射影的ユニタリ表現 $\mathsf{f}_1 \overline{\otimes} \cdots \overline{\otimes} \mathsf{f}_n$ は条件 **GM1** を満たす．また，この表現は射影 $P_1 \otimes \cdots \otimes P_n$ に関して条件 **GM4** を満たす．よって，補題 3.5.6 より題意を得る．□

以下，$E_{G,2}(\rho)$ の計算について重要な定理を紹介する．

定理 3.5.9　([69, 51])　$\mathcal{H}_j = \mathcal{H}$ であり，$\mathcal{H}^{\otimes n}$ 上の純粋状態 $|\phi\rangle$ がテンソルの順番に関する置換 $\sigma \in S_n$ の作用について不変であるとする．このとき，

$$\max_{|a\rangle\langle a| \in \mathrm{SEP}} |\langle a|\phi\rangle|^2 = \max_{|b\rangle \in \mathcal{H}: \|b\|=1} |\langle b^{\otimes n}|\phi\rangle|^2 \tag{3.16}$$

が成り立つ.

定理 3.5.10　([68])　それぞれの系 $\mathcal{H}_j$ の基底 $\{|e_{j,k}\rangle\}$ から，合成系 $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ 上の基底 $\{|e_{1,k_1}\rangle \otimes \cdots \otimes |e_{n,k_n}\rangle\}_{k_1,\ldots,k_n}$ を考える．合成系上の状態 ρ を上記の基底について行列表示したとき，全ての行列成分が非負の実数であるとする．このとき，任意の状態 ρ' について $E_{G,2}(\rho \otimes \rho') = E_{G,2}(\rho) + E_{G,2}(\rho')$ が成り立つ.

例 3.5.11　(最大エンタングル状態)　2 体系で $\mathcal{H}_1 = \mathcal{H}_2 = \mathbb{C}^r$ のとき，最大エンタングル状態 $\frac{1}{\sqrt{r}}|I\rangle\rangle$ は $E_{G,2}(\frac{1}{\sqrt{r}}|I\rangle\rangle) = \log r$ を満たす．$\mathrm{U}(r)$ の基本表現とその複素共役表現のテンソル積表現は条件 **GM1**,**GM4** を満たす．したがって，補題 3.5.6 より，(3.15) が成り立つ．さらに，補題 3.5.10 および補題 3.5.7 より，

$$\begin{aligned}
&R_{L,g,\infty}\left(\frac{1}{\sqrt{r}}|I\rangle\rangle\right) = E_{R,\infty}\left(\frac{1}{\sqrt{r}}|I\rangle\rangle\right) = E_{R,s,\infty}\left(\frac{1}{\sqrt{r}}|I\rangle\rangle\right) \\
&= E_{G,1,\infty}\left(\frac{1}{\sqrt{r}}|I\rangle\rangle\right) = E_{G,2,\infty}\left(\frac{1}{\sqrt{r}}|I\rangle\rangle\right) = E_{G,2}\left(\frac{1}{\sqrt{r}}|I\rangle\rangle\right),\ 1 > \forall s > 0
\end{aligned} \tag{3.17}$$

が成り立つ.

例 3.5.12　(2 体系の純粋状態)　$n = 2$ とし，$\mathcal{H}_1 \otimes \mathcal{H}_2$ 上の純粋状態 $|A\rangle\rangle$ に注目し，その Schmidt 分解を $\sum_{j=1}^{k} \sqrt{d_j}|v_j\rangle \otimes |u_j\rangle$ とする．$d_1 \geq d_2 \geq$

$\cdots \geq d_k$ とする．この純粋状態の系 $\mathcal{H}_1$ についての縮約密度行列は $\rho := \sum_{j=1}^k d_j^2 |v_j\rangle\langle v_j|$ とする．このとき，$\max_{\rho_1 \in \mathrm{SEP}} \mathrm{Tr}\, |A\rangle\rangle\langle\langle A|\rho_1 = d_1$ を得る．したがって，$E_{G,1}(|A\rangle\rangle) = E_{G,2}(|A\rangle\rangle) = -\log d_1$ を得る．さらに，後に示すように，

$$\min_{\rho_1 \in \mathrm{SEP}} \mathrm{Tr}\, |A\rangle\rangle\langle\langle A|^{1-s} \rho_1^s = (\mathrm{Tr}\, \rho^{\frac{1}{1-s}})^{1-s}, \quad 0 > s > -1 \tag{3.18}$$

$$\max_{\rho_1 \in \mathrm{SEP}} \mathrm{Tr}\, |A\rangle\rangle\langle\langle A|^{1-s} \rho_1^s = (\mathrm{Tr}\, \rho^{\frac{1}{1-s}})^{1-s}, \quad 1 > s > 0 \tag{3.19}$$

が成り立つ．したがって，$E_{R,1-s}(|A\rangle\rangle) = H_{\frac{1}{1-s}}(\rho)$ を得る．さらに，$s \to 0$ の極限を考えると，$E_R(|A\rangle\rangle) = H(\rho)$ を得る．(3.11) の第一不等式と (3.18) での $s \to -1$ の極限を組み合わせると，$R_{L,g}(|A\rangle\rangle) \geq H_{\frac{1}{2}}(\rho)$ を得る．実は，以下に示すように $R_L(|A\rangle\rangle) \leq H_{\frac{1}{2}}(\rho)$ が成り立つので [119]，以下を得る．

$$R_L(|A\rangle\rangle) = R_{L,g}(|A\rangle\rangle) = H_{\frac{1}{2}}(\rho). \tag{3.20}$$

(3.20) の証明. $R = (\sum_{j=1}^k \sqrt{d_j})^2$ とし，セパラブル状態 $\rho^- := \frac{1}{R-1} \sum_{j \neq l} \sqrt{d_j}\sqrt{d_l} |v_j\rangle\langle v_j| \otimes |u_l\rangle\langle u_l|$ に注目する．以下では，

$$\begin{aligned}
\rho^+ :=& \frac{|A\rangle\rangle\langle\langle A| + (R-1)\rho^-}{R} \\
=& \sum_{j,l} \frac{\sqrt{d_j d_l}}{R} |v_j\rangle\langle v_l| \otimes |u_j\rangle\langle u_l| + \sum_{j \neq l} \frac{\sqrt{d_j d_l}}{R} |v_j\rangle\langle v_j| \otimes |u_l\rangle\langle u_l|
\end{aligned}$$

がセパラブルであることを示す．このために，$\alpha_j = 2\alpha_{j-1} + 1, \alpha_0 = 0$ となるように，$\alpha_0, \ldots, \alpha_k$ を定義する．そして，$|e_t\rangle := \sum_{j=1}^k (\frac{d_j}{R})^{1/4} e^{\frac{i2\pi}{\alpha_k}\alpha_j t} |v_j\rangle$，$|e_t^*\rangle := \sum_{j=1}^k (\frac{d_j}{R})^{1/4} e^{-\frac{i2\pi}{\alpha_k}\alpha_j t} |u_j\rangle$ としたとき，$\sum_{t=1}^{\alpha_k} |e_t\rangle\langle e_t| \otimes |e_t^*\rangle\langle e_t^*|$ が ρ^+ に等しいことを示す．

$$\begin{aligned}
&\langle v_j| \otimes \langle u_l| \sum_{t=1}^{\alpha_k} |e_t\rangle\langle e_t| \otimes |e_t^*\rangle\langle e_t^*| |v_{j'}\rangle \otimes |u_{l'}\rangle \\
&= \frac{(d_j d_l d_{j'} d_{l'})^{1/4}}{R} \sum_{t=1}^{\alpha_k} e^{\frac{i2\pi}{\alpha_k}(\alpha_j - \alpha_l - \alpha_{j'} + \alpha_{l'})t}
\end{aligned}$$

となる．右辺の値が 0 になるのは，$\alpha_j - \alpha_l - \alpha_{j'} + \alpha_{l'}$ が 0 とならないときのみである．この値が 0 になるための必要十分条件は $j = l$, $j' = l'$ または $j = j'$, $l = l'$ となるときである．したがって，$\sum_{t=1}^{\alpha_k} |e_t\rangle\langle e_t| \otimes |e_t^*\rangle\langle e_t^*|$ は ρ^+ に一致する．すなわち，ρ^+ はセパラブルである．よって，$R_L(|A\rangle\rangle) \le 2\psi(1/2|\rho) = H_{\frac{1}{2}}(\rho)$ が成り立つので，(3.20) を得る．□

(3.18) の証明.　ρ_1 をセパラブル状態とする．定理 3.4.1 より，$\mathrm{Tr}_2\,\rho_1 \otimes I_2 \ge \rho_1$ となる．$0 > s > -1$ について，$x \mapsto -x^s$ は行列単調であるので，$\rho' := \mathrm{Tr}_2\,\rho_1$ とすると，$\rho_1^s \ge (\mathrm{Tr}_2\,\rho_1 \otimes I_2)^s = {\rho'}^s \otimes I_2$ が成り立つ．したがって (2.23) より

$$\begin{aligned}\mathrm{Tr}\,\rho_1^s |A\rangle\rangle\langle\langle A|^{1-s} &= \mathrm{Tr}\,\rho_1^s |A\rangle\rangle\langle\langle A| \ge \mathrm{Tr}\,{\rho'}^s \otimes I_2 |A\rangle\rangle\langle\langle A| \\ &= \mathrm{Tr}\,{\rho'}^s \rho \ge (\mathrm{Tr}\,\rho^{\frac{1}{1-s}})^{1-s}\end{aligned}$$

を得る．状態 $\frac{\rho^{\frac{1}{1-s}}}{\mathrm{Tr}\,\rho^{\frac{1}{1-s}}}$ を $\sum_j d_j' |v_j\rangle\langle v_j|$ と対角化し，$v_j' := \frac{Av_j}{\|Av_j\|}$ とする．すると，$\rho_1 = \sum_j d_j' |v_j\rangle\langle v_j| \otimes |v_j'\rangle\langle v_j'|$ のとき等号が成り立つ．よって (3.18) を得る．□

(3.19) の証明.　ρ_1 をセパラブル状態とする．定理 3.4.1 より，$\mathrm{Tr}_2\,\rho_1 \otimes I_2 \ge \rho_1$ となる．$1 > s > 0$ について，$x \mapsto x^s$ は行列単調であるので，$\rho' := \mathrm{Tr}_2\,\rho_1$ とすると，$\rho_1^s \le (\mathrm{Tr}_2\,\rho_1 \otimes I_2)^s = {\rho'}^s \otimes I_2$ が成り立つ．したがって (2.24) より

$$\begin{aligned}\mathrm{Tr}\,\rho_1^s |A\rangle\rangle\langle\langle A|^{1-s} &= \mathrm{Tr}\,\rho_1^s |A\rangle\rangle\langle\langle A| \le \mathrm{Tr}\,{\rho'}^s \otimes I_2 |A\rangle\rangle\langle\langle A| \\ &= \mathrm{Tr}\,{\rho'}^s \rho \le (\mathrm{Tr}\,\rho^{\frac{1}{1-s}})^{1-s}\end{aligned}$$

を得る．(3.18) の証明と同じように $\rho_1 = \sum_j d_j' |v_j\rangle\langle v_j| \otimes |v_j'\rangle\langle v_j'|$ のとき等号が成り立つ．よって (3.19) を得る．□

例 3.5.13（Dicke 状態 [51, 68]）　$\mathcal{H}_i = \mathbb{C}^r$ とする．和が n となる r 個の非負の整数からなるベクトル $\boldsymbol{n} = (n_1, \ldots, n_r)$ に対して，**Dicke 状態**

$$|\boldsymbol{n}; \mathrm{Dicke}\rangle := \sum_{(\omega_1,\ldots,\omega_n)\in T_{\boldsymbol{n}}} \frac{1}{\sqrt{|T_{\boldsymbol{n}}|}} |\omega_1\rangle \otimes \cdots \otimes |\omega_n\rangle$$

を定義する．ここで，$T_{\boldsymbol{n}}$ は $\{1,\ldots,r\}^n$ の要素でその成分に $1 \le j \le r$ が含まれる数が n_j となるものの集合である．以下，$E_{G,2}(|\boldsymbol{n}\rangle)$ を計算する．定理3.5.9が適用でき，(3.16)の右辺に問題が帰着できる．さらに，(3.16)の右辺に現れるベクトルは，最大化問題の性質から，計算基底についての成分が正の値のものに制限できる．確率分布を与えるベクトル $\boldsymbol{p} = (p_1,\ldots,p_r)$ に対して，$|\boldsymbol{p}\rangle := \sum_{j=1}^r \sqrt{p_j}|j\rangle$ とすると，

$$\begin{aligned}\langle \boldsymbol{p}|^{\otimes n}|\boldsymbol{n}; \mathrm{Dicke}\rangle &= \sqrt{|T_{\boldsymbol{n}}|}\prod_{j=1}^{r}\sqrt{p_j}^{n_j} = \sqrt{|T_{\boldsymbol{n}}|}e^{\frac{n}{2}\sum_{j=1}^r \frac{n_j}{n}\log p_j} \\ &= \sqrt{|T_{\boldsymbol{n}}|}e^{\frac{n}{2}(-H(\frac{\boldsymbol{n}}{n})-D(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p}))} \le \sqrt{|T_{\boldsymbol{n}}|}e^{\frac{n}{2}-H(\frac{\boldsymbol{n}}{n})}\end{aligned}$$

となる．$\boldsymbol{p} = \frac{\boldsymbol{n}}{n}$ のとき等号が成り立つので，$E_{G,2}(|\boldsymbol{n}; \mathrm{Dicke}\rangle) = nH(\frac{\boldsymbol{n}}{n}) - \log|T_{\boldsymbol{n}}|$ を得る．次に定理3.5.5が適用できることを示し，(3.15)を示す．$\mathrm{U}(1)^r$ を $\mathrm{U}(r)$ の部分群 $\{\sum_{j=1}^r e^{i\theta_j}|j\rangle\langle j|\}$ として埋め込む．f を $U(r)$ の基本表現とし，$\mathsf{f}_{(1,0,\ldots,0)}^{\otimes n}$ を $U(1)^r$ に制限したものを考える．この表現の下で，条件**GM1**が成り立つ．$|\frac{\boldsymbol{n}}{n}\rangle$ は条件**GM2**を満たし，対称テンソル積空間に注目すると，条件**GM3′**も満たす．したがって，補題3.5.6より，(3.15)が成り立つ．

さらに，補題3.5.10より，$E_{G,2}(|\boldsymbol{n}; \mathrm{Dicke}\rangle^{\otimes m}) = m(nH(\frac{\boldsymbol{n}}{n}) - \log|T_{\boldsymbol{n}}|)$ を得る．よって補題3.5.7より，$|\boldsymbol{n}\rangle$ は(3.17)を満たす．

例 3.5.14 (Stabilizer 状態[51]) $(\mathbb{C}^q)^{\otimes r} := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_r$ 上に $\mathbb{F}_q^{2r}$ の離散Heisenberg表現 $\mathsf{W}_{\mathbb{F}_q}^r$ が与えられた場合を考える．$\mathbb{F}_q^{2r}$ の狭義自己直交部分群 N のStabilizer状態と離散Heisenberg表現 $\mathsf{W}_{\mathbb{F}_q}^r$ を N に制限したものは**GM1, GM4**を満たす．したがって，補題3.5.6より，N のStabilizer状態は(3.5.5)を満たす．

例 3.5.15 (反対称状態[51, 68]) $\mathcal{H}_i = \mathbb{C}^r$, $n \le r$ とし，P を反対称テンソル積空間への射影とする．このとき，状態 $\frac{P}{\mathrm{Tr}\,P}$ を**反対称状態**とよぶ．反対称テンソル積空間の性質より，$\|P|a_1 \otimes \cdots \otimes a_n\rangle\| \le \frac{1}{\sqrt{n!}}\|a_1 \otimes \cdots \otimes a_n\|$ となり，$a_1,\ldots,a_n$ が互いに直交するときのみ等号が成立する．したがって，$\max_{|a\rangle\langle a|\in\mathrm{SEP}}\langle a|P|a\rangle = \max_{|a\rangle\langle a|\in\mathrm{SEP}}\langle a|P^2|a\rangle = \frac{1}{n!}$ となる．

さらに，$\mathrm{U}(r)$ の n 回テンソル積表現は条件 **GM1**，**GM4** を満たす．補題 3.5.6 より，

$$R_{L,g}\left(\frac{P}{\mathrm{Tr}\,P}\right)=E_R\left(\frac{P}{\mathrm{Tr}\,P}\right)=E_{R,s}\left(\frac{P}{\mathrm{Tr}\,P}\right)=E_{G,1}\left(\frac{P}{\mathrm{Tr}\,P}\right)=\log n!,\quad 1>\forall s>0$$

が成り立つ．

しかし，行列 P の行列成分は非負ではないので，定理 3.5.10 は適用できず，別途 $E_{G,2}(\frac{P^{\otimes 2}}{(\mathrm{Tr}\,P)^2})$ を計算する必要がある．行列 $P^{\otimes 2}$ は置換群の作用に関して，不変であるので定理 3.5.9 が適用でき，$\max_{|a\rangle\langle a|\in\mathrm{SEP}}\langle a|P^{\otimes 2}|a\rangle = \max_{\mathrm{Tr}\,A^\dagger A=1}\langle\langle A^{\otimes n}|P^{\otimes 2}|A^{\otimes n}\rangle\rangle$ を得る．$A^\dagger A$ の固有値を $a_1,\ldots,a_r$ とすると，P と $A^{\dagger\otimes n}$ との可換性より，$\langle\langle A^{\otimes n}|P^{\otimes 2}|A^{\otimes n}\rangle\rangle = \mathrm{Tr}\,A^{\dagger\otimes n}PA^{\otimes n}P^T = \mathrm{Tr}\,PA^\dagger A^{\otimes n} = \sum_{1\le j_1<\ldots<j_n\le r} a_{j_1}\cdots a_{j_n}$ を得る．この値は $a_1,\ldots,a_r$ についての Schur 関数であるので，例 2.3.5 より，Schur 凹関数となり，条件 $\sum_{j=1}^r a_j = 1$ の下での最大値は $a_j = \frac{1}{r}$ のときに達成される．したがって，等式 $\max_{|a\rangle\langle a|\in\mathrm{SEP}}\langle a|P^{\otimes 2}|a\rangle = \frac{r!}{r^n n!(r-n)!}$ を得る．補題 3.5.7 が適用できるので，

$$\begin{aligned}R_{L,g}\left(\frac{P^{\otimes 2}}{(\mathrm{Tr}\,P)^2}\right) &= E_R\left(\frac{P^{\otimes 2}}{(\mathrm{Tr}\,P)^2}\right) = E_{R,s}\left(\frac{P^{\otimes 2}}{(\mathrm{Tr}\,P)^2}\right) = E_{G,1}\left(\frac{P^{\otimes 2}}{(\mathrm{Tr}\,P)^2}\right)\\ &= \log\frac{r^n n!(r-n)!}{r!} < 2\log n!,\quad 1>\forall s>0\end{aligned}$$

を得る．このように，反対称状態の場合は加法性は成り立たない．

3.5.3　PPT 状態に基づく拡張

2 体系の場合，すなわち，$n=2$ の場合には，$E[f]_{1,2}$ の定義で考えた最小化の範囲をセパラブル状態の集合 SEP から PPT 状態の集合 PPT に置き換えることが可能である．置き換えて得られた量を $E[f]_{1,2}^{\mathrm{PPT}}$ と記す．合成系上の量子通信路 Λ が与えられたとき，任意の PPT 状態 ρ について，$\Lambda(\rho)$ が PPT 状態となるとき，量子通信路 Λ を **PPT 量子通信路**とよぶ．補題 3.5.1 の証明と同様にして，PPT 量子通信路 Λ は

$$E[f]_{1,2}^{\mathrm{PPT}}(\Lambda(\rho)) \le E[f]_{1,2}^{\mathrm{PPT}}(\rho) \tag{3.21}$$

を満たす．また，セパラブルな量子通信路 Λ は PPT 量子通信路となることが確認できる．そのため，セパラブルな量子通信路 Λ は (3.21) を満たす．すなわち，$E[f]_{1,2}^{\mathrm{PPT}}$ はセパラブルエンタングルメント単調となる．同様に，$R_{L:1,2}$, $R_{L,g:1,2}$ の定義においても SEP を PPT に置き換えることが可能となり，置き換えて得られる量を $R_{L:1,2}^{\mathrm{PPT}}$, $R_{L,g:1,2}^{\mathrm{PPT}}$ と記すことにする．これらの量は同じように，セパラブルエンタングルメント単調となる．また，PPT 量子通信路 Λ の下で，(3.21) を満たす量を **PPT 単調**とよぶことにする．

定理 3.4.1 での (2)⇒(3) の証明.　f が相対エントロピーであるときの $E[f]_{1,2}^{\mathrm{PPT}}$ に注目する．このとき，$E[f]_{1,2}^{\mathrm{PPT}}(\rho) = 0$ となることと ρ が PPT 状態であることは同値である．また，関数 $\rho \mapsto E[f]_{1,2}^{\mathrm{PPT}}(\rho)$ は連続である．PPT 状態 ρ と LOCC 操作 Λ_n の系列を考える．$E[f]_{1,2}^{\mathrm{PPT}}(\Lambda_n(\rho^{\otimes n})) = 0$ である．したがって，$\Lambda_n(\rho^{\otimes n})$ がある状態 ρ_0 に収束するとすると連続性より，$E[f]_{1,2}^{\mathrm{PPT}}(\rho_0) = 0$ である．一方，$(\mathbb{C}^2)^{\otimes 2}$ 上の最大エンタングル状態 $|\Phi\rangle\langle\Phi|$ は $E[f]_{1,2}^{\mathrm{PPT}}(|\Phi\rangle\langle\Phi|) > 0$ を満たす．したがって，**(3)** を得る．　□

3.6　エンタングルメントの定量化 II：操作的方法

3.6.1　2 体系の場合

上記の議論では，幾何学的にどの程度セパラブル状態から離れているか測ることで，エンタングルメントを定量化した．しかし，このような議論からでは，与えられたエンタングル状態がエンタングルした資源としてどの程度の能力を持っているかわからない．1 つの方法は，2 体系に限ることになるが，最大エンタングル状態をどれだけ抽出できるか定量的に測る方法である．この方法では，最初に 2 つの系 $\mathcal{H}_A$, $\mathcal{H}_B$ が状態 ρ に準備されたとき，我々の操作を LOCC に限り，その終状態が可能な限りサイズの大きい最大エンタングル状態に十分近くなるようにする．しかし，単一の系ではシンプルな解析ができないので，2 つの系 $\mathcal{H}_A^{\otimes n}$, $\mathcal{H}_B^{\otimes n}$ が状態 ρ の n 階テンソル積状態 $\rho^{\otimes n}$ となる場合を考え，n が大きくなる漸近極限を考える．この設定では，初めにターゲットとなる最大エンタングル状態に対応する 2 つの量子系 $\mathcal{H}_{A,n}$, $\mathcal{H}_{B,n}$ を考える．ここで，$\mathcal{H}_{B,n}$ は $\mathcal{H}_{A,n}$ と同型とし，その次元を d_n とする．そし

て，ターゲットとなる最大エンタングル状態は $|X_n\rangle := \frac{1}{\sqrt{d_n}}|I\rangle\rangle$ で与えられるとする．合成系 $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ から合成系 $\mathcal{H}_{A,n} \otimes \mathcal{H}_{B,n}$ へのLOCC量子通信路 Λ_n を用いて，初期状態 $\rho^{\otimes n}$ を変化させる．このとき，このプロトコルは $\Phi_n := (|X_n\rangle, \Lambda_n)$ で記述され，その性能はサイズ $|\Phi_n| := d_n$ とターゲットとなる状態と終状態との忠実度から決まる量 $\epsilon(\Phi_n) := 1 - \langle X_n|\Lambda_n(\rho^{\otimes n})|X_n\rangle$ を用いて評価される．したがって，漸近的に $\epsilon(\Phi_n)$ が0に収束する条件の下で，1つのエンタングル状態 ρ あたりの最大エンタングル状態の生成レート $\lim_{n\to\infty} \frac{\log|\Phi_n|}{n}$ がどこまで大きくできるか考える．この最大値を $E_D(\rho)$ [3] と記し，**エンタングルメント蒸留**とよぶ．すなわち，エンタングルメント蒸留 $E_D(\rho)$ は以下のように定義される．

$$E_D(\rho) := \sup_{\{\Phi_n\}} \left\{ \limsup_{n\to\infty} \frac{\log|\Phi_n|}{n} \middle| \lim_{n\to\infty} \epsilon(\Phi_n) = 0 \right\}.$$

このように，エンタングルメント蒸留 $E_D(\rho)$ はエンタングル状態 ρ が資源としてどれだけのエンタングルメントを持っているか測る量である．

次に，特定のエンタングル状態 ρ をLOCCから生成するために，どれだけの最大エンタングル状態をコストとして必要であるか考える．エンタングルメント蒸留の場合と同様に，ターゲットとなる状態として，n 階テンソル積状態 $\rho^{\otimes n}$ となる場合を考え，n が大きくなる漸近極限を扱う．初めに，コストとして消費される最大エンタングル状態 $|X_n\rangle$ とその状態が含まれる合成系 $\mathcal{H}_{A,n} \otimes \mathcal{H}_{B,n}$ を考え，そのサイズを d_n とする．合成系 $\mathcal{H}_{A,n} \otimes \mathcal{H}_{B,n}$ から合成系 $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ へのLOCC量子通信路 Λ_n 状態 $|X_n\rangle$ を変化させる．このとき，このプロトコルは $\Psi_n := (|X_n\rangle, \Lambda_n)$ で記述され，その性能はサイズ $|\Psi_n| := d_n$ とターゲットとなる状態と終状態との忠実度から決まる量 $\epsilon(\Psi_n) := 1 - F(\Lambda_n(|X_n\rangle\langle X_n|), \rho^{\otimes n})$ を用いて評価される．したがって，漸近的に $\epsilon(\Phi_n)$ が0に収束する条件の下で，1つのエンタングル状態 ρ あたりの必要となる最大エンタングル状態のレート $\lim_{n\to\infty} \frac{\log|\Phi_n|}{n}$ がどこまで小さくできるか考える．この最小値を $E_C(\rho)$ [3] と記し，**エンタングルメントコスト**とよぶ．すなわち，エンタングルメントコスト $E_C(\rho)$ は以下のように定義される．

$$E_C(\rho) := \inf_{\{\Psi_n\}} \left\{ \liminf_{n\to\infty} \frac{\log|\Psi_n|}{n} \middle| \lim_{n\to\infty} \epsilon(\Psi_n) = 0 \right\}.$$

このように，エンタングルメントコスト $E_C(\rho)$ は，エンタングル状態 ρ の生成にどれだけの資源を消費するか測る量である．

エンタングルメントコスト $E_C(\rho)$ とエンタングルメント蒸留 $E_D(\rho)$ の意味を考えると，以下の関係が成り立つ．

$$E_D(\rho) \le E_C(\rho). \tag{3.22}$$

この関係式は以下のように考えると導出できる．最初に，ある一定サイズの最大エンタングル状態を準備し，エンタングルメントコストの限界を達成するLOCC 量子通信路を用いて，量子状態 $\rho^{\otimes n}$ に変換し，その後に，エンタングルメント蒸留の限界を達成する LOCC 量子通信路を用いて，最大エンタングル状態に変換する．この 2 つの処理を合わせた処理は LOCC 量子通信路であるので，終状態となる最大エンタングル状態のサイズは初期状態となる最大エンタングル状態のサイズよりも小さい．したがって，(3.22) が導ける．

さらに，以下の式が成り立つ．

$$E_D(\rho) \le E_R(\rho) \le E_C(\rho). \tag{3.23}$$

ρ が純粋状態の場合は ρ_A を $|X\rangle$ の系 $\mathcal{H}_A$ 上の縮約密度行列とすると，$E_R(|X\rangle)$ は $H(\rho_A)$ であった．実は，以下が成り立つ [3]．

$$E_D(|X\rangle) = E_R(|X\rangle) = E_C(|X\rangle) = H(\rho_A). \tag{3.24}$$

$E_D(|X\rangle) \ge H(\rho_A)$ となることは，6.5 節で述べるプロトコルから確認できる．$E_F(|X\rangle) \le H(\rho_A)$ [3] の証明は割愛する．詳しくは [38] などを参照のこと．

3.6.2 多体系の場合

多体系の場合については，残念ながら上記のような意味で操作的にエンタングルメントを定量化する方法は十分進んでいない．局所性条件を課した場合での状態識別とエンタングルの定量化とは以下に述べるような関係がある．

多体系 $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ 上の状態 ρ に対して以下の量を考える．

$$L(\rho) := \max_L \{L \mid \exists L, \exists \rho_1, \ldots, \rho_L, \exists M = \{M_j\}_{j=1}^L \text{ s.t. } \operatorname{Tr} M_j \rho_j = 1\}.$$

ただし，M は セパラブル POVM に限られ，ρ_j は ρ とエンタングル状態として同値なものに限られる．

定理 3.6.1 ([50])　D を合成系 $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ の次元とすると，$\log \frac{D}{L(\rho)} \geq R_{L,g}(\rho)$ が成り立つ．

証明.　$L(\rho) = L$ の定義の条件を満たす $\rho_1, \ldots, \rho_N$ およびセパラブル POVM $M = \{M_j\}_{j=1}^{L}$ を選ぶ．このとき，$\mathrm{Tr}\, M_j \leq \frac{D}{L(\rho)}$ となる j が存在する．$1 + t = \mathrm{Tr}\, M_j$ とすると，$\rho'_j := \frac{M_j - \rho_j}{t}$ は状態となる．そして，$\frac{M_j}{\mathrm{Tr}\, M_j} = \frac{\rho_j + t\rho'_j}{1+t}$ は separable 状態となり，題意を得る．　□

特に，ρ が狭義自己直交部分群 N の Stabilizer 状態の場合，N の部分群 N' でその要素がセパラブル POVM によって同時測定可能なものに注目する．N' によって識別可能な N の Stabilizer 状態の数を L とすると，$L(\rho) \geq L$ を得る．特に，グラフ状態の場合はグラフの点を辺で繋がった2つの点が異なる色になるように白，黒の2色に色分けできた場合は，以下のように，$L(\rho)$ の下限が得られる．点 j が白のとき，$e_j \in \mathbb{F}_2^{2r}$ を第 j 番目のみが 1 となり，他の成分が 0 となるベクトルとする．点 j が黒のとき，$e_j \in \mathbb{F}_2^{2r}$ を第 $r+j$ 番目のみが 1 となり，他の成分が 0 となるベクトルとする．$e_1, \ldots, e_r$ から生成される $\mathbb{F}_2^{2r}$ の部分群 N'' と N の交わり $N' := N \cap N''$ の要素が同時測定可能である．黒の点の数と白の点の数の多い方を m とすると，N' の要素の数は 2^m となる．したがって，N' によって識別可能な Stabilizer 状態の数は 2^m となる．

色分けに3色以上必要な場合は，もう少しややこしい．最も点が多い色の点について上の白と同じ方法で e_j を定義し，残りの点については e_j を上の黒と同じ方法で定義する．最も点が多い色の点の数を m とすると，同じ議論により，N' によって識別可能な Stabilizer 状態の数は 2^m となる．

この事実と (3.10) を組み合わせることで，いくつかのグラフ状態について，$R_{L,g}$, $E_{G,1}$ が求まる．

例 3.6.2 (1D Cluster 状態 [82])　n 個の点からなる 1D Cluster 状態 ρ の場合，図 3.1 の左側のように2色に色分けできる．この場合，上記の値 m は $\lceil \frac{n}{2} \rceil$ となる．したがって，$R_{L,g}(\rho)$ の下限 $\log \frac{2^{\lceil \frac{n}{2} \rceil}}{2^n} = \lfloor \frac{n}{2} \rfloor \log 2$ を得る．一方，n 個の点を図 3.1 の左側のように2つのグループ S, S^c に分けることができる．この2つのグループから2体系のエンタングルメントに注目した場合，それぞれのグループの内部での C-NOT は局所ユニタリと見なされる．したがって，

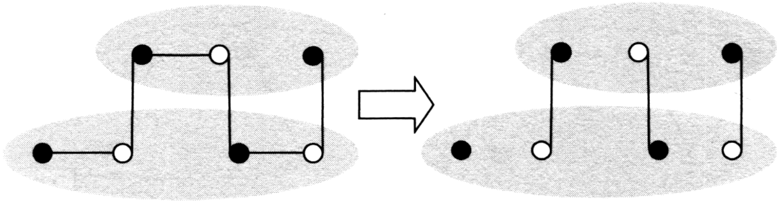


図 3.1 1D Cluster 状態

図 3.1 の右側のように，それぞれのグループの内部で点線の部分の辺について C-NOT を施すと，$E_{G,1:S,S^c}(\rho) = \lfloor \frac{n}{2} \rfloor \log 2$ を得る．したがって，(3.10) を用いると，$R_{L,g}(\rho) = E_{G,1}(\rho) = \lfloor \frac{n}{2} \rfloor \log 2$ を得る．

例 3.6.3 (Ring 状態 [82]) n が偶数の場合 n 個の点からなる Ring 状態 ρ の場合，図 3.2 の最初の図のように 2 色に色分けできる．この場合，上記の値 m は $\frac{n}{2}$ となる．n が奇数の場合 n 個の点からなる Ring 状態 ρ の場合，図 3.3 の最初の図のように白，黒，グレーの 3 色に色分けできる．この場合，上記の値 m は $\lceil \frac{n}{2} \rceil$ となる．したがって，$R_{L,g}(\rho)$ の下限 $\log \frac{2^{\lceil \frac{n}{2} \rceil}}{2^n} = \lfloor \frac{n}{2} \rfloor \log 2$ を得る．

n が偶数の場合，n 個の点を図 3.2 の最初の図のように 2 つのグループ S, S^c に分けることができる．そして，図 3.2 の矢印 1 に従って，グループ内で複数の C-NOT を施す．そして，図 3.2 の矢印 2 に従って，local complementation を施し，最後に，図 3.2 の矢印 3 に従って，グループ内で複数の C-NOT を施す．すると，$E_{G,1:S,S^c}(\rho) = \frac{n}{2} \log 2$ を得る．したがって，(3.10) を用いると，$R_{L,g}(\rho) = E_{G,1}(\rho) = \frac{n}{2} \log 2$ を得る．

n が奇数の場合，n 個の点を図 3.3 の最初の図のように 2 つのグループ S, S^c に分けることができる．そして，先と同じように，矢印の順序で変換することで，$E_{G,1:S,S^c}(\rho) = \lfloor \frac{n}{2} \rfloor \log 2$ を得る．この場合，残念ながら上限と下限は一致しない．

例 3.6.4 (GHZ 状態 [82]) n 個の点からなる GHZ 状態 ρ の場合，対応するグラフは星グラフである．このグラフは図 3.4 の左側のように 2 色に色分けでき，上記の値 m は 1 となる．一方，n 個の点を図 3.4 の左側のように 2 つのグループ S, S^c に分けることができる．そして，グループ内で複数の C-NOT

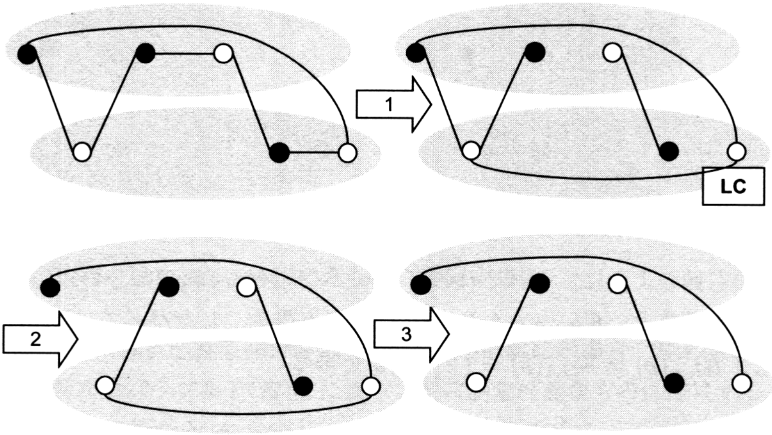


図 **3.2**　偶数の場合の Ring 状態

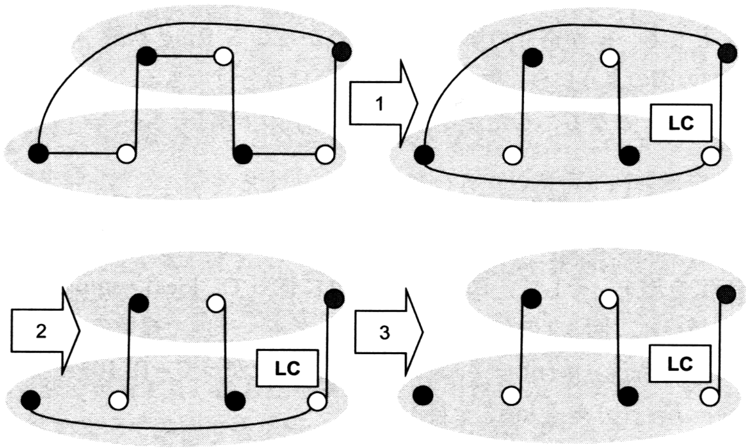


図 **3.3**　奇数の場合の Ring 状態

を施すことで，$E_{G,1:S,S^c}(\rho) = \log 2$ を得る．したがって，(3.10) を用いると，$R_{L,g}(\rho) = E_{G,1}(\rho) = \log 2$ を得る．

その他，2D Cluster 状態の場合についても，この方法で得られる上限と下限が一致することが知られている [82]．

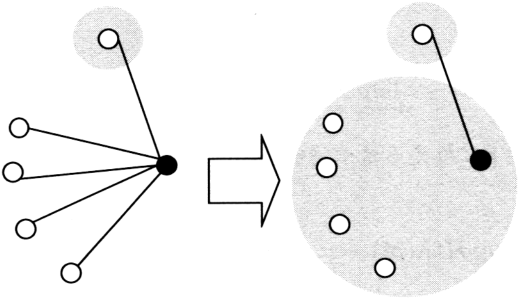


図 3.4　GHZ 状態

3.7　エンタングルメントの定量化 III：凸分解を用いた手法

3.6 節の議論から，2 体系の場合，純粋状態の場合には縮約密度行列のエントロピーをエンタングルメントの基準として用いることが適切であると考えることができる．以下では，2 体系に限って議論を進める．そのため，ρ が純粋状態の場合にのみ定義される関数 $E(\rho)$ を $H(\mathrm{Tr}_B\,\rho)$ で与える．しかし，一般の混合状態の場合には (3.23) において必ずしも等号が成り立つとは限らない．そのため他の基準を考える必要がある．ここで，2.3.1 項で定義した convex roof を適用する．すなわち，$E(\rho)$ の convex roof として，**エンタングルメントフォーメーション** $E_f(\rho) := \mathrm{CR}(E)(\rho)$ [5] を定義する．すると，補題 3.5.2 より，$E_R(\rho)$ は凸関数であるから，補題 2.3.2 を適用すると $E_R(\rho) \le E_f(\rho)$ を得る．ここで ρ についての参照系 $\mathcal{H}_C$ を与え，その純粋状態化を $|\sqrt{\rho}\rangle\rangle$ とすると，(1.4) の議論から POVM を用いた表式

$$E_f(\rho) = \min_{\{M_j\}:\mathrm{POVM}} \sum_j (\mathrm{Tr}\, M_j\rho) E\left(\frac{\sqrt{\rho}M_j\sqrt{\rho}}{\mathrm{Tr}\, M_j\rho}\right) \tag{3.25}$$

を得る．

$E(\rho)$ が加法性を満たすことから，convex roof の定義より，

$$E_f(\rho_1 \otimes \rho_2) \le E_f(\rho_1) + E_f(\rho_2) \tag{3.26}$$

を得る．一般に，この等式が成り立つか否かについては加法性問題として長年量子情報理論の未解決問題であったが，Hastings[34] により否定的に解決された．すなわち，(3.26) において一般には等号は成り立たない．

そして以下の定理が知られている．

定理 3.7.1 （[3, 55]）

$$\lim_{n\to\infty}\frac{1}{n}E_f(\rho^{\otimes n}) = E_C(\rho). \tag{3.27}$$

一方，E_f は以下に与える量子通信路 Λ の **Holevo 容量** $\chi(\Lambda)$ [63] と密接な関係がある．

$$\chi(\Lambda) := \sup_{\rho} H(\Lambda(\rho)) - \min_{(p_j,\rho_j):\sum_j p_j\rho_j=\rho}\sum_j p_j H(\Lambda(\rho_j)). \tag{3.28}$$

環境系を $\mathcal{E}$ とし，等長写像を U とする Λ の Stinespring 表現を考える．(3.28) の第 2 項は合成系 $\mathcal{K}\otimes\mathcal{E}$ 上の状態 $U\rho U^\dagger$ のエンタングルメントフォーメーションと一致する [86]．すなわち，

$$\chi(\Lambda) = \sup_{\rho} H(\Lambda(\rho)) - E_f(U\rho U^\dagger). \tag{3.29}$$

$E_f(\rho)$ の計算であるが，群論的な対称性がある場合は，以下のようにその計算が単純になる．

補題 3.7.2 群 G の系 $\mathcal{H}_A$, $\mathcal{H}_B$ への射影的ユニタリ表現 f_A, f_B が与えられたとき，系 $\mathcal{H}_A\otimes\mathcal{H}_B$ のテンソル積表現 $\mathsf{f}_A\otimes\mathsf{f}_B$ に関する既約空間を 1 つ選び，$\mathcal{H}_C$ と記し，$\mathcal{H}_C$ 上の完全混合状態を ρ_C と記す．このとき以下を得る．

$$E_f(\rho_C) = \min_{|x\rangle\in\mathcal{H}_C,\ \|x\|=1} H(\mathrm{Tr}\,|x\rangle\langle x|). \tag{3.30}$$

証明. 初めに，convex roof の定義から (3.30) の $\geq$ を得る．

さらに，任意の $|x\rangle\in\mathcal{H}_C$ と $g\in G$ に対して，

$$H(\mathrm{Tr}\,|x\rangle\langle x|) = H(\mathsf{f}_A(g)\,\mathrm{Tr}\,|x\rangle\langle x|\mathsf{f}_A(g^{-1}))$$

が成り立つ．さらに，$\int_G \mathsf{f}_A\otimes\mathsf{f}_B(g)|x\rangle\langle x|\mathsf{f}_A\otimes\mathsf{f}_B(g^{-1})\mu(dg)$ は ρ_C に等しい．したがって，(3.30) において $\leq$ を得る．□

さらに，忠実度から定義される量 $1-F^2$ から定義されるエンタングルメント量 $E[1-F^2]$ について以下の定理が成り立つ．

定理 3.7.3 （[110]）　$E[1-F^2]$ は自己 convex roof となる．すなわち，$E[1-F^2](\rho) = \mathrm{CR}(E[1-F^2]_{\mathcal{P}(\mathcal{H})})$ が成り立つ．

第 4 章

群共変性と最適情報処理

4.1　共変的状態族と最適測定

量子情報処理の枠組みでは，できるだけエラーの少ない情報処理が求められる．そのような場合，エラーを与える関数を数学的に定式化し，その値を最適化（最小化）する処理が望ましいと考えられる．本章では，最適測定を含め，群論的対称性がある様々な設定の下で，最適な処理のスキームを与える．また，これらの解析を通じて，量子論的な情報処理の限界を明らかにする．

4.1.1　共変的状態族と共変的測定

我々の欲しい情報が値をとる集合 Θ が群 G の作用に関して閉じている場合を考えよう [62]．群 G が Θ に推移的に作用しているとすると，G の適当な部分群 H を選ぶと，$\Theta \cong G/H$ となる．このような情報 $\theta \in \Theta$ で記述されている状態はどのような密度行列 ρ_θ であろうか？　群 G の Hilbert 空間 $\mathcal{H}$ への（射影的）ユニタリ表現 f が与えられているとする．すると，

$$\mathsf{f}(g)\rho_\theta \mathsf{f}(g)^\dagger = \rho_{g\theta}$$

を満たすとき，状態族 $\{\rho_\theta \,|\, \theta \in \Theta\}$ は表現 f に関して**共変的**であるという．ここで，Θ のある 1 点（以下**原点**とよぶ）$\theta_0 \in \Theta$ を固定する．すると，群 G は推移的に作用しているので，任意の $\theta \in \Theta$ に対して，$\theta = g(\theta)\theta_0$ となる $g(\theta) \in G$ がとれる．したがって，上の条件は $\rho_\theta = \mathsf{f}(g(\theta))\rho_{\theta_0}\mathsf{f}(g(\theta))^\dagger$ に変形

できる．固定化群 H について，

$$\mathsf{f}(h)\rho_0\mathsf{f}(h)^\dagger = \rho_0, \quad \forall h \in H \tag{4.1}$$

となる密度行列 ρ_0 を与えると，f に関して共変的状態族は

$$\rho_\theta = \mathsf{f}(g(\theta))\rho_0\mathsf{f}(g(\theta))^\dagger \tag{4.2}$$

で与えられる．

例えば，共変的状態族の例として，群 G が SU(2) の場合に，最大ウェイトが λ となる既約表現空間 $\mathcal{U}_\lambda$ 上の共変的状態族を考えよう．$\mathcal{U}_\lambda$ への既約表現を f_λ とし，$\mathfrak{su}(2)$ の要素 $F_1^z := \frac{1}{2}\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$ を用いて部分群 H を $H = \{\exp(tF_1^z)\}_{t\in\mathbb{R}}$ で定める．$|\lambda : \zeta\rangle$ を複素数 ζ で特徴付けられるコヒーレントベクトルとすると，コヒーレント状態 $\rho_\zeta := |\lambda : \zeta\rangle\langle\lambda : \zeta|$ は，$\Theta = \hat{\mathbb{C}}$（リーマン球面）とすると H を固定化群とする共変的状態族となる．このとき，$\mathsf{f}_\lambda(g(\zeta))$ は $U_{\zeta,t}$ となる．

同様に群 G が $\mathrm{S\tilde{U}(1,1)}$ の場合に，最大ウェイトが λ となる既約表現空間 $\mathcal{U}_\lambda$ 上の共変的状態族を考えよう．このとき，$\mathfrak{su}(1,1)$ の要素 $F_{-1}^z := \frac{1}{2}\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$ を用いて部分群 H を $H = \{\exp(tF_{-1}^z)\}_{t\in\mathbb{R}}$ で定める．$|\lambda : \zeta\rangle$ を複素数 ζ で特徴付けられるコヒーレントベクトルとすると，コヒーレント状態 $\rho_\zeta := |\lambda : \zeta\rangle\langle\lambda : \zeta|$ は，$\Theta = D$（単位円板）とすると H を固定化群とする共変的状態族となる．このとき，同様に，$\mathsf{f}_\lambda(g(\zeta))$ は $U_{\zeta,t}$ となる．これら2つの例における詳しい記号の使い方については [37] の 4.2 節を見よ．

Heisenberg 群 $H(2,\mathbb{R})$ の場合，1モードの Bose 粒子系 $L^2(\mathbb{R})$ 上のコヒーレントベクトル $||\zeta\rangle$ を用いて，コヒーレント状態 $\rho_\zeta := |\zeta\rangle\langle\zeta|$ を与えると，コヒーレント状態は共変的状態族となる．

一般の Lie 群 G の場合，最大ウェイトはベクトル $\boldsymbol{\lambda}$ で与えられ，その最大ウェイトを持つ既約表現空間 $\mathcal{U}_{\boldsymbol{\lambda}}$ 上の共変的状態族を考えよう．ウェイトが $\boldsymbol{\lambda}$ となる最大ウェイトベクトル $|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle$ の G による軌道は複素数に値を持つベクトル ζ を用いて記述され，コヒーレント状態 $\rho_\zeta = |\boldsymbol{\lambda} : \zeta\rangle\langle\boldsymbol{\lambda} : \zeta|$ として与えられる．すると，コヒーレント状態の集合は $H = \{g \in G | \mathsf{f}(g)|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|\mathsf{f}(g)^\dagger =$

$|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|\}$ を固定化群とする共変的状態族となる．この部分についての記号については，[37] の 5.7, 5.9, 5.10 節を参照のこと．

次に，系 $\mathcal{H}$ の状態が未知であるが，上記の共変な状態族 $\{\rho_\theta|\theta \in \Theta\}$ のどれかであることがわかっているとして，そのパラメータを推測する問題を考えよう．この場合，Θ に値を持つ POVM M を用いて測定することになる．以下では，Θ に値を持つ POVM の集合を $\mathcal{M}(\Theta)$ と記す．なお，パラメータ空間 Θ は一般には連続値であるので，連続値の POVM の定義 **(M1)**, **(M2)**, **(M3)** に基づいて議論を進める．そして，推測値 $\hat{\theta}$ が真の値 θ から外れた場合，そのエラーの度合いを表す**エラー関数** $R(\theta,\hat{\theta})$ を考えよう．以下の議論では，エラー関数の期待値 $\mathcal{D}_{R,\theta}(M) := \int_\Theta R(\theta,\hat{\theta}) \operatorname{Tr} M(d\hat{\theta})\rho_\theta$ を小さくする推定方法を考える．ただ，議論によっては，エラー関数の符号を逆にして定義される**利得関数**の期待値を大きくする推定方法を考えることもある．上記の期待値を小さくしたい場合については，R を誤差関数とよび，大きくしたい場合は，R を利得関数とよぶ．

しかし，θ そのものはどの値をとるかわからないので，θ に依存した量で POVM の性能を測ることはできない．したがって，最悪の値 $\mathcal{D}_R(M) := \max_{\theta\in\Theta} \mathcal{D}_{R,\theta}(M)$ に注目しよう．最適な POVM を求めるために，このような基準を最小化する POVM を求める手法を mini-max 法とよぶ．一方，ある Θ 上の確率分布 ν （Bayes 事前分布とよぶ）を仮定し，その期待値 $\mathcal{D}_{R,\nu}(M) := \int_\Theta \mathcal{D}_{R,\theta}(M)\nu(d\hat{\theta})$ を最小化する方法を Bayes 法とよぶ．このとき，

$$\mathcal{D}_R(M) \geq \mathcal{D}_{R,\nu}(M) \tag{4.3}$$

が成り立つ．ここで，2 つの POVM M_0, M_1 と $0 < p < 1$ に対して，新たな POVM M_p を $M_p(B) := (1-p)M_0(B) + pM_1(B)$ で定義する．すると，$\mathcal{D}_{R,\theta}(M_p) = (1-p)\mathcal{D}_{R,\theta}(M_0) + p\mathcal{D}_{R,\theta}(M_1)$ が成り立つ．さらに，ν について平均をとると，

$$\mathcal{D}_{R,\nu}(M_p) = (1-p)\mathcal{D}_{R,\nu}(M_0) + p\mathcal{D}_{R,\nu}(M_1) \tag{4.4}$$

が成り立つ．

Θ が等質空間であるので，θ と $\hat{\theta}$ の差は $g\theta$ と $g\hat{\theta}$ の差と同じであると考えることが自然である．よって，エラー関数 R は以下の**群不変性**を満たすと仮

定することは自然である.

$$R(\theta,\hat{\theta}) = R(g\theta, g\hat{\theta}). \tag{4.5}$$

一方，Θ に値を持つ $\mathcal{H}$ 上の POVM M が条件 $M(gB) = \mathsf{f}(g)M(B)\mathsf{f}(g)^\dagger$ を満たすとき，表現 f に関して**共変的**という．ただし，$gB := \{g\theta \mid \theta \in B\}$ である．$\hat{\theta}' := g\hat{\theta}$ とすると，この条件は $M(d\hat{\theta}') = \mathsf{f}(g)M(d\hat{\theta})\mathsf{f}(g)^\dagger$ と同値である．Θ に値を持つ共変的な POVM の集合を $\mathcal{M}_{\mathrm{cov}}(\Theta)$ と記すことにする．また，その端点の集合を $\mathcal{M}_{\mathrm{cov,ex}}(\Theta)$ と記すことにする．

R が不変性 (4.5) を満たし，POVM M が共変的であるとき，$\hat{\theta}' := g^{-1}\hat{\theta}$ とすると，

$$\begin{aligned}\mathcal{D}_{R,g\theta}(M) &= \int_\Theta R(g\theta,\hat{\theta}) \operatorname{Tr} M(d\hat{\theta})\rho_{g\theta} = \int_\Theta R(g\theta,\hat{\theta}) \operatorname{Tr} M(d\hat{\theta})\mathsf{f}(g)\rho_\theta \mathsf{f}(g)^\dagger \\ &= \int_\Theta R(g\theta, g\hat{\theta}') \operatorname{Tr} M(d\hat{\theta}')\rho_\theta = \mathcal{D}_{R,\theta}(M)\end{aligned}$$

が成り立つ．したがって，$\mathcal{D}_{R,\theta}(M) = \mathcal{D}_R(M) = \mathcal{D}_{R,\nu}(M)$ が成り立つ．さらに，以下の定理が成り立つ．

定理 4.1.1（量子 Hunt-Stein の定理 [62]）　Θ はコンパクトであるとする．

$$\begin{aligned}\min_{M\in\mathcal{M}(\Theta)} \mathcal{D}_R(M) &= \min_{M\in\mathcal{M}(\Theta)} \mathcal{D}_{R,\mu_\Theta}(M) = \min_{M\in\mathcal{M}_{\mathrm{cov}}(\Theta)} \mathcal{D}_R(M) \\ &= \min_{M\in\mathcal{M}_{\mathrm{cov}}(\Theta)} \mathcal{D}_{R,\mu}(M) = \min_{M\in\mathcal{M}_{\mathrm{cov,ex}}(\Theta)} \mathcal{D}_{R,\mu_\Theta}(M).\end{aligned}$$

すなわち，mini-max 法の解と，不変測度 μ_Θ による Bayes 法の最適値は一致し，最適な POVM は共変的 POVM で与えられる．また，mini-max 法の解を与える POVM は群共変的である．

なお，上の定理は，共変的でない POVM が Bayes 法の最適値を与えないことを意味しているわけでない．事実，Bayes 法の最適値を与え，共変的でない POVM が存在する．

証明.　(4.3) より，任意の POVM M に対して，以下を満たす共変的 POVM $\bar{M}$ が存在することを示せば十分である．

$$\mathcal{D}_R(M) \ge \mathcal{D}_{R,\mu_\Theta}(M) = \mathcal{D}_{R,\mu_\Theta}(\bar{M}).$$

このために，任意の $g \in G$ に対して，POVM M_g を $M_g(B) := \mathsf{f}(g)^\dagger M(gB)\mathsf{f}(g)$ で定義する．すると，$\mathcal{D}_{R,\theta}(M_g) = \mathcal{D}_{R,g\theta}(M)$ が成り立つ．よって，θ について積分すると，μ_Θ の不変性より，$\mathcal{D}_{R,\mu_\Theta}(M_g) = \mathcal{D}_{R,\mu_\Theta}(M)$ が成り立つ．また POVM $\bar{M} := \int_G M_g \mu_G(dg)$ は共変的となり，(4.4) より，$\mathcal{D}_{R,\mu_\Theta}(\bar{M}) = \int_G \mathcal{D}_{R,\mu_\Theta}(M_g)\mu_G(dg) = \mathcal{D}_{R,\mu_\Theta}(M)$ となり，題意が示せる．なお，$\min_{M\in\mathcal{M}_{\mathrm{cov,ex}}(\Theta)} \mathcal{D}_{R,\mu_\Theta}(M)$ と等しくなることは，(4.4) より確認できる． □

Θ がコンパクトでない場合は，不変測度 μ の積分が有限値ではないので，上記の定理は Bayes 法については成立しないが，mini-max 法については成立する．すなわち以下を得る．

定理 4.1.2 （[95, 9]） Θ は局所コンパクトであるとする．共変的な POVM M に対して $\mathcal{D}_R(M) = \mathcal{D}_{R,\theta}(M)$ が成り立つ．さらに，$\min_{M\in\mathcal{M}(\Theta)} \mathcal{D}_R(M) = \min_{M\in\mathcal{M}_{\mathrm{cov}}(\Theta)} \mathcal{D}_R(M) = \min_{M\in\mathcal{M}_{\mathrm{cov,ex}}(\Theta)} \mathcal{D}_R(M)$ が成り立ち，共変測定により最適な測定が与えられる．

注意 4.1.3 推定の一般的な設定では，必ずしも，状態を記述するパラメータ空間 Θ の全ての情報を推定することが求められているとは限らない．Θ についての部分的な情報だけ求められていることも多い．その場合，推定したい部分的なパラメータの集合を Θ_1 とし，Θ_1 に対しても群 G の作用が定義されているとする．このとき真の値 $\theta \in \Theta$ と推定値 $\theta_1 \in \hat{\Theta}$ に対して定義される誤差関数 $R(\theta, \hat{\theta})$ に対しても，群不変性

$$R(\theta, \hat{\theta}) = R(g\theta, g\hat{\theta}), \quad g \in G \tag{4.6}$$

を定義することができる．この一般的な定義の下，定理 4.1.1 とまったく同じ主張が成り立つ．

このような一般的な設定では，Θ, Θ_1 には群 G の作用が定義されているものの，等質空間とはならないことが多い．例えば，群 G の作用の下で Θ_1 の要素が動かない場合は，すなわち，

$$g\hat{\theta} = \hat{\theta}, \quad \forall g \in G, \forall \hat{\theta} \in \Theta_1 \tag{4.7}$$

となる場合が考えられる．この場合，Θ_1 が 1 点からなる集合でない限り，等質空間とはならない．この例では，共変的測定 $\{M_{\hat{\theta}}\}_{\hat{\theta}\in\Theta_1}$ は以下を満たすもの

として与えられる.

$$\mathsf{f}(g)M_{\hat{\theta}}\mathsf{f}(g)^\dagger = M_{\hat{\theta}}, \quad \forall g \in G, \forall \hat{\theta} \in \Theta_1. \tag{4.8}$$

4.1.2　共変的測定の特徴付け

次に，Θ が等質空間である場合に，共変的測定がどのように記述できるか考えよう．そして，原点 $\theta_0 \in \Theta$ に対応する POVM の要素 $T := M_{\theta_0}$ に注目する．すると，

$$M_\theta = \mathsf{f}(g(\theta))T\mathsf{f}(g(\theta))^\dagger \tag{4.9}$$

となり，T だけから共変的 POVM が定まる．次に T が満たすべき条件を調べよう．Θ の θ_0 での固定化群 H について，

$$\mathsf{f}(h)T\mathsf{f}(h)^\dagger = T, \quad \forall h \in H \tag{4.10}$$

が成り立つ．さらに，全積分が単位行列になることから，

$$\int_\Theta \mathsf{f}(g(\theta))T\mathsf{f}(g(\theta))^\dagger \mu_\Theta(d\theta) = \int_G \mathsf{f}(g)T\mathsf{f}(g)^\dagger \mu_G(dg) = I \tag{4.11}$$

となる．すなわち，$T \geq 0$ から，(4.9) によって群共変測定が与えられるための必要十分条件は (4.10) と (4.11) で与えられる．以下では，条件 (4.10) と (4.11) を満たす共変的 POVM を M_T と記し，T が**生成する**共変的 POVM とよぶことにする．

注目している表現空間が既約空間 $\mathcal{U}_\lambda$ で与えられる場合を考える．以下では，一般に群 G の既約ユニタリ表現を表すラベルの集合を $\hat{G}$ とし，その要素を $\lambda \in \hat{G}$ と記述する．これは Lie 群の場合，最大ウェイトがそれに対応する既約表現のラベルとして機能するからである．この場合，対応する既約ユニタリ表現を f_λ と記載する．一般の群について，既約ユニタリ表現のラベルを表すときは $\lambda \in \hat{G}$ と記述し，一般の Lie 群で，最大ウェイトで既約ユニタリ表現を指定する場合については，$\boldsymbol{\lambda}$ と記述する．ただし，SU(2), SU(1,1) のように，最大ウェイトが1つの実数で記述できる場合は，λ と記述する．

固定化群 H の $\mathcal{U}_\lambda$ への表現が完全可約であり，その既約分解が $\bigoplus_m \mathcal{H}_m \otimes \mathbb{C}^{n_{\lambda,m}}$ で与えられる場合，$T \geq 0$ が群共変的測定を与えるための条件 (4.10) は

$\mathbb{C}^{n_{\lambda,m}}$ 上の半正定値作用素 T_m を用いて,

$$T = \bigoplus_m I_m \otimes T_m \tag{4.12}$$

と書けることと同値である．ここで，I_m は $\mathcal{H}_m$ 上の単位作用素である．この事実は，H の表現に対して完全可約な場合の Schur の補題 ([37] の補題 2.3.5) を適用することで確認できる．以下では G がコンパクトであり，$\mathcal{U}_\lambda$ が有限次元となり，その次元が d_λ である場合を考える．μ_G は正規化された不変測度であるので，$T \geq 0$ が群共変測定を与えるためのもう 1 つの条件 (4.11) は

$$\mathrm{Tr}\, T = d_\lambda \tag{4.13}$$

に置き換えられる．この事実は $\int_G \mathsf{f}_\lambda(g) T \mathsf{f}_\lambda(g)^\dagger \mu_G(dg)$ は $\mathsf{f}_\lambda(g)$ と可換になり，Schur の補題より I のスカラー倍になることから確かめられる．一方，G が非コンパクトであるがユニモジュラーである場合，$\|v\| = 1, \|u\| = 1$ に対して,

$$d_\lambda^{-1} := \int_G |\langle v|\mathsf{f}_\lambda(g)|u\rangle|^2 \mu_G(dg) < \infty \tag{4.14}$$

が成り立つ場合を考える．このとき，d_λ は形式的次元（詳しくは [37] の 3.7 節を参照のこと）とよばれ，条件 (4.11) は $\mathrm{Tr}\, T = d_\lambda$ に置き換えられる．もし，部分群 H が単位元だけからなる群とすると，(4.12) は自明な条件となり，(4.13) のみ調べれば十分である．

次に，群 G の表現 f_λ が完全可約であり，表現空間 $\mathcal{H}$ の既約分解が $\bigoplus_\lambda \mathcal{U}_\lambda \otimes \mathbb{C}^{n_\lambda}$ で与えられる場合を，2 つの step に分けて扱う．そのために，$\mathcal{U}_\lambda \otimes \mathbb{C}^{n_\lambda}$ への射影を P_λ と記す．最初に，各既約成分 $\mathcal{U}_\lambda$ は条件 (4.14) を満たす場合について考える．ここで，部分群 H が単位元だけからなる群とする．条件 (4.10) は自明な条件となり，条件 (4.11) のみ検討すれば十分である．したがって，$T \geq 0$ が群共変測定を与えるための条件 (4.11) は

$$\mathrm{Tr}_{\mathcal{U}_\lambda} P_\lambda T P_\lambda = d_\lambda I_{n_\lambda} \tag{4.15}$$

と同値である．ここで，I_{n_λ} は $\mathbb{C}^{n_\lambda}$ 上の単位行列である．

次に，固定化群 H が一般の部分群となる場合を考える．表現空間 $\mathcal{H}$ への部分群 H の表現についての既約分解は $\bigoplus_m \mathcal{H}_m \otimes \mathbb{C}^{\sum_\lambda n_\lambda n_{\lambda,m}}$ で与えられる．

このとき，$T \geq 0$ が群共変測定を与えるための条件 (4.10) は $\mathbb{C}^{\sum_\lambda n_\lambda n_{\lambda,m}}$ 上の半正定値作用素 T_m を用いて，

$$T = \bigoplus_m I_m \otimes T_m \tag{4.16}$$

と書けることと同値である．この条件は，条件 (4.12) と同じである．そして，条件 (4.11) は先に与えた (4.15) と同値である．

なお，これまでの議論は Lie 群 G の代わりに Lie 環 $\mathfrak{g}$ と等質空間 Θ が与えられれば十分である．Lie 環 $\mathfrak{g}$ を用いた方が，Lie 群 G を用いるよりも議論がすっきりする場合があるので，必要に応じて，Lie 環 $\mathfrak{g}$ を用いた議論を行うこととする．

4.1.3　共変的測定の最適化

次に，G が Lie 群の場合に具体的な設定の下で，最適測定を導出しよう．そのために，誤差関数 $R(\theta, \hat{\theta})$ の選び方について述べる．状態推定の設定では，ある状態族 $\{\rho_{1,\theta}\}$ を考え，$\rho_{1,\theta}$ と同一にある系が複数独立に準備される設定を考えることが多い．この場合，合成系の状態は $\rho_{1,\theta}^{\otimes n}$ となり，ρ_θ として，$\rho_{1,\theta}^{\otimes n}$ を選んだ状態族 $\{\rho_{1,\theta}^{\otimes n}\}$ の推定を考えることになる．あくまでも知りたいのは，状態族 $\{\rho_{1,\theta}\}$ の要素であるため，誤差関数 $R(\theta, \hat{\theta})$ は状態族 $\{\rho_{1,\theta}\}$ に基づいて与えられる．このように，一般に状態推定では，誤差関数 $R(\theta, \hat{\theta})$ を与える状態族 $\{\rho_{1,\theta}\}$ と物理的に準備される状態族 $\{\rho_\theta\}$ が異なることが多い．

よく用いられる誤差関数に Bures の距離の 2 乗 $1 - \mathrm{Tr}\,|\sqrt{\rho_\theta}\sqrt{\rho_{\hat{\theta}}}|$ が挙げられる．しかし，これを用いた場合の計算が難しいこともあるので，$1 - \mathrm{Tr}\,\rho_\theta \rho_{\hat{\theta}}$ を用いることもある．他に，測定値が集合 $\{\hat{\theta} \mid \mathrm{Tr}\,\rho_\theta \rho_{\hat{\theta}} \leq \epsilon\}$ に含まれる確率（以下，**ϵ-誤差確率**とよぶ）を誤差関数として注目することもある．この場合，誤差関数は $R(\theta, \hat{\theta})$ は θ がこの集合に含まれる場合は，1 と定義し，それ以外の場合は 0 であるとする．以下では，主に状態族 $\{\rho_{1,\theta}\}, \{\rho_\theta\}$ が最高ウェイト $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}$ を持つ既約表現のコヒーレント状態として与えられる場合を考え，最適な測定を行ったときの ϵ-誤差確率を $P_{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}, \epsilon}$ と記すことにする．

そして，以下の定理が成り立つ．

定理 4.1.4　Lie 環 $\mathfrak{g}$ が $\mathfrak{su}(2), \mathfrak{su}(1,1)$ で与えられ，表現空間が $\mathcal{U}_\lambda$ であるとする．このとき，コヒーレント状態族 $\{\rho_\zeta := |\lambda : \zeta\rangle\langle\lambda : \zeta|\}_\zeta$ に対して，誤

差関数 $R(\zeta,\hat{\zeta})$ が忠実度 $|\langle\lambda:\zeta|\lambda:\hat{\zeta}\rangle|^2$ の単調減少関数で与えられているとき，最適測定を与える共変的 POVM は $T=d_\lambda|\lambda;\lambda\rangle\langle\lambda;\lambda|$ によって与えられる．ただし，$\mathfrak{su}(1,1)$ の場合は，$\lambda<-\frac{1}{2}$ とする．

一方，$\mathfrak{g}$ が $\mathfrak{h}(2,\mathbb{R})$ であり，コヒーレント状態族 $\{\rho_\zeta:=|\zeta\rangle\langle\zeta|\}_\zeta$ に対して，誤差関数 $R(\zeta,\hat{\zeta})$ が忠実度 $|\langle\zeta|\hat{\zeta}\rangle|^2$ の単調減少関数で与えられている場合は，最適測定を与える共変的 POVM は $T=|0\rangle\langle 0|$ によって与えられる．

証明. 最初に単調減少関数 f を $R(\zeta,\hat{\zeta})=\mathsf{f}(|\langle\lambda:\zeta|\lambda:\hat{\zeta}\rangle|^2)$ となるように選ぶ．定理 4.1.1 より，任意の $M\in\mathcal{M}_{\mathrm{cov,ex}}(\Theta_s)$ について，

$$\int \mathsf{f}(|\langle\lambda:\zeta|\lambda:\hat{\zeta}\rangle|^2)\langle\lambda;\lambda|M(d\hat{\zeta})|\lambda;\lambda\rangle$$
$$\geq\int \mathsf{f}(|\langle\lambda;\zeta|\lambda:\hat{\zeta}\rangle|^2)\langle\lambda;\lambda|M_{d_\lambda|\lambda;\lambda\rangle\langle\lambda;\lambda|}(d\hat{\zeta})|\lambda;\lambda\rangle$$

を示せば十分である．ゆえに，題意を示すには，任意の実数 $c\in[0,1]$ に対して定義される集合 $\mathcal{R}_c:=\{\zeta\,|\,|\langle\lambda;\zeta|\lambda;\lambda\rangle|^2\geq c\}$ について，不等式

$$\int_{R_c}\langle\lambda;\lambda|M(d\hat{\zeta})|\lambda;\lambda\rangle\geq\int_{R_c}\langle\lambda;\lambda|M^{d_\lambda|\lambda;\lambda\rangle\langle\lambda;\lambda|}(d\hat{\zeta})|\lambda;\lambda\rangle \tag{4.17}$$

を示せば十分である．

以下，$\mathfrak{su}(2)$, $\mathfrak{su}(1,1)$ の場合について示す．$|\lambda;m\rangle$ をウェイト m を持つ $\mathcal{U}_\lambda$ の要素とする．(4.12) より，$M=M_{d_\lambda|\lambda;m\rangle\langle\lambda;m|}$ の場合に，(4.17) を示せば十分である．$|\langle\lambda:\zeta|\lambda;m\rangle|^2$ は $x:=|\hat{\zeta}|^2$ にのみ依存することから，$c=(1+sx_c)^{-2\lambda}=|\langle\lambda:\zeta|\lambda;\lambda\rangle|^2$ となるように，x_c を選び，関数 $h(x):=\frac{|\langle\lambda;m|\lambda:\sqrt{x}\rangle|^2}{|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2}$ を用いると，

$$\int_{R_c}d_\lambda|\langle\lambda;m|U_{\hat{\zeta},s}|\lambda;\lambda\rangle|^2\mu_{\Theta_s}(d\hat{\zeta})=\int_{R_c}d_\lambda|\langle\lambda;m|\lambda:\hat{\zeta}\rangle|^2\mu_{\Theta_s}(d\hat{\zeta})$$
$$=\int_0^{x_c}d_\lambda|\langle\lambda;m|\lambda:\sqrt{x}\rangle|^2\frac{da}{(1+sx)^2}=\int_0^{x_c}h(x)d_\lambda|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2\frac{dx}{(1+sx)^2}$$

を得る．したがって，

$$\int_0^{x_c}d_\lambda|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2\frac{dx}{(1+sx)^2}\geq\int_0^{x_c}h(x)d_\lambda|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2\frac{dx}{(1+sx)^2} \tag{4.18}$$

を示せば十分である．そして，

$$h(x) = \frac{|\langle\lambda;m|\lambda:\sqrt{x}\rangle|^2}{|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2} = \left|\langle\lambda;m|\frac{(\sqrt{x}\mathsf{K}_{-,s})^{\lambda-m}}{(\lambda-m)!}|\lambda;\lambda\rangle\right|^2$$
$$= x^{\lambda-m}\left|\langle\lambda;m|\frac{(\mathsf{K}_{-,s})^{\lambda-m}}{(\lambda-m)!}|\lambda;\lambda\rangle\right|^2$$

が成り立つことから，$h(x)$ は x に関して単調増加となる．よって，$h(x_c) \le 1$ であれば，(4.18) が成り立つ．

一方 $h(x_c) > 1$ であっても，

$$x_m = \begin{cases} \infty & s = 0, 1 \\ 1 & s = -1 \end{cases}$$

とすると，

$$\int_{x_c}^{x_m} d_\lambda|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2 \frac{dx}{(1+sx)^2} \le \int_{x_c}^{x_m} h(x) d_\lambda|\langle\lambda;\lambda|\lambda:\sqrt{x}\rangle|^2 \frac{dx}{(1+sx)^2}$$

は成り立つ．したがって，全積分が1であるから (4.18) が成り立つ．

一方 Lie 環 $\mathfrak{g}$ が Heisenberg 群の Lie 環 $\mathfrak{h}(2,\mathbb{R})$ の場合，最高ウェイトを (λ_Z, λ_F) とし，x_c を $c = e^{x_c} = |\langle\sqrt{\lambda_Z}\zeta|0\rangle|^2$ となるように選ぶ．このとき，ウェイトベクトルは個数ベクトル $|m\rangle$ であるので，上記の証明において，ベクトル $|\lambda;m\rangle$ を $|m\rangle$ に置き換え，関数 $h(x)$ を以下で与える．

$$h(x) := \frac{|\langle m|\sqrt{\lambda_Z}\sqrt{x}\rangle|^2}{|\langle 0|\sqrt{\lambda_Z}\sqrt{x}\rangle|^2} = \left|\langle m|\frac{(\sqrt{\lambda_Z}\sqrt{x}\mathsf{a}^\dagger)^m}{m!}|0\rangle\right|^2$$
$$= x^m\lambda_Z^m\left|\langle m|\frac{(\mathsf{a}^\dagger)^m}{m!}|0\rangle\right|^2$$

が x に関して単調増加であるので，同じようにして示せる．　□

例 4.1.5　$\mathfrak{g} = \mathfrak{su}(2), \mathfrak{su}(1,1)$ の場合について，最適な測定を行ったときの ϵ-誤差確率 $P_{\lambda_1,\lambda,\epsilon}$ を求めよう．$\lambda < \frac{-1}{2}$ または，正の半整数とすると，$\zeta = re^{i\theta}$，$x = (1+sr^2)$ とし，r_0 を $(1+sr^2)^{-2\lambda_1} = \epsilon$ を満たすものとすると，

$$P_{\lambda_1,\lambda,\epsilon} = s(2\lambda+1)\int_{\{(1+s|\zeta|^2)^{-2\lambda_1}\le\epsilon\}} (1+s|\zeta|^2)^{-2\lambda}\mu_{\Theta_s}(d\zeta)$$

$$= (2\lambda+1)\int_{r_0}^{a}(1+sr^2)^{-2\lambda}\frac{2\pi srdr}{\pi(1+sr^2)^2}$$

$$= (2\lambda+1)\int_{\epsilon^{\frac{-1}{2\lambda_1}}}^{b} x^{-2\lambda-2}dx = -[x^{-2\lambda-1}]_{\epsilon^{\frac{-1}{2\lambda_1}}}^{b} = \epsilon^{\frac{2\lambda+1}{2\lambda_1}}$$

を得る．ここで，$s=1$ のときは，$a=\infty, b=\infty$ であり，$s=-1$ のときは，$a=1, b=0$ である．特に，$\lambda = n\lambda_1$ のときは，$\epsilon^{n+\frac{1}{2\lambda_1}}$ となり，n が大きくなると，指数的に 0 に収束する．

例 4.1.6 $\mathfrak{g} = \mathfrak{h}(2,\mathbb{R}) \rtimes \mathfrak{u}(1)$ の場合について，最適な測定を行ったときの ϵ-誤差確率 $P_{\lambda_1,\lambda,\epsilon}$ を求めよう．$\lambda_1 = (\lambda_{1,Z}, \lambda_{1,F})$, $\lambda = (\lambda_Z, \lambda_F)$, $\zeta = re^{i\theta}$ とし，r_0 を $e^{-\lambda_{1,Z} r_0^2} = \epsilon$ を満たすものとすると，

$$P_{\lambda_1,\lambda,\epsilon} = \lambda_Z \int_{\{e^{-\lambda_{1,Z}|\zeta|^2} \le \epsilon\}} e^{-\lambda_Z|\zeta|^2}\mu_{\mathbb{C}}(d\zeta) = \lambda_Z \int_{r_0}^{\infty} e^{-\lambda_Z r^2}\frac{2\pi rdr}{\pi}$$

$$= -[e^{\lambda_Z r^2}]_{r_0}^{\infty} = \epsilon^{\frac{\lambda_Z}{\lambda_{1,Z}}}$$

を得る．特に，$\lambda = n\lambda_1$ のときは，ϵ^n となり，n が大きくなると，指数的に 0 に収束する．

定理 4.1.4 は以下のように一般化できる．

定理 4.1.7 一般の Lie 環 $\mathfrak{g}$ に対して，最高ウェイトが $\boldsymbol{\lambda}$ となる既約表現空間 $\mathcal{U}_{\boldsymbol{\lambda}}$ への歪エルミート表現 $\mathsf{f}_{\boldsymbol{\lambda}}$ を考える．この表現上 コヒーレント状態族 $\{\rho_\zeta := |\boldsymbol{\lambda} : \zeta\rangle\langle\boldsymbol{\lambda} : \zeta|\}_\zeta$ に対して，原点 $|\boldsymbol{\lambda},\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda},\boldsymbol{\lambda}|$ を不変にする不変部分群 H_1 の Lie 環 $\mathfrak{h}_1$ が $\mathfrak{su}(d)$ または $\mathfrak{u}(d)$ とする．（一般の Lie 環に対するコヒーレント状態の定義については [37] の 5.5, 5.8, 5.9 節を参照のこと．）このとき，$\mathfrak{g}$ は $\mathfrak{h}_1 \oplus \mathfrak{p}$ と直和分解でき，$\mathfrak{p}$ は $\mathfrak{h}_1$ の自然な作用に関して閉じている．$\mathfrak{h}_1$ の $\mathfrak{p}$ への表現が複素化可能であり，$\mathfrak{su}(d)$ または $\mathfrak{u}(d)$ の $\mathbb{C}^d$ への自然な表現と同型であるとする．このとき，コヒーレント状態族 $\{\rho_\zeta := |\boldsymbol{\lambda};\zeta\rangle\langle\boldsymbol{\lambda};\zeta|\}_\zeta$ は $\mathbb{C}^d$ の要素でパラメトライズされる．そして，誤差関数 $R(\zeta,\hat{\zeta})$ が忠実度 $|\langle\boldsymbol{\lambda} : \zeta|\boldsymbol{\lambda} : \hat{\zeta}\rangle|^2$ の単調減少関数で与えられているとき，最適測定は，共変的 POVM $M_{d_{\boldsymbol{\lambda}}|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|}$ で与えられる．ただし，$\mathfrak{g}$ が非コンパクトの場合，形式的次元 $d_{\boldsymbol{\lambda}}$ が存在するとする．

この条件は Lie 群 G が $\mathrm{SU}(d)$ であり，最高ウェイト $\boldsymbol{\lambda} = [m, 0, \ldots, 0]$ の場合のコヒーレント状態は $\mathfrak{h}_1$ が $\mathfrak{u}(d-1)$ となり，条件を満たす．すなわち，群が $\mathrm{SU}(d)$ であり，$\boldsymbol{\lambda} = [m, 0, \ldots, 0]$ の場合については，定理 4.1.7 の仮定が成り立つ [39]．他に，Heisenberg 群とユニタリ群の半直積 $\mathrm{H}(2r, \mathbb{R}) \rtimes \mathrm{U}(r)$ の $L^2(\mathbb{R}^r)$ への自然な表現（[37] の 6.3 節を参照）によるコヒーレント状態も条件を満たす．

証明.　最初に単調減少関数 f を $R(\zeta, \hat{\zeta}) = \mathsf{f}(|\langle \boldsymbol{\lambda} : \zeta | \boldsymbol{\lambda} : \hat{\zeta} \rangle|^2)$ となるように選ぶ．定理 4.1.1 より，任意の $M \in \mathcal{M}_{\mathrm{cov,ex}}(\Theta)$ について，

$$\int \mathsf{f}(|\langle \boldsymbol{\lambda} : \zeta | \boldsymbol{\lambda} : \hat{\zeta} \rangle|^2) \langle \boldsymbol{\lambda}; \boldsymbol{\lambda} | M_T(d\hat{\zeta}) | \boldsymbol{\lambda}; \boldsymbol{\lambda} \rangle$$
$$\geq \int \mathsf{f}(|\langle \boldsymbol{\lambda} : \zeta | \boldsymbol{\lambda} : \hat{\zeta} \rangle|^2) \langle \boldsymbol{\lambda}; \boldsymbol{\lambda} | M^{d_{\boldsymbol{\lambda}} |\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|}(d\hat{\zeta}) | \boldsymbol{\lambda}; \boldsymbol{\lambda} \rangle$$

を示せば十分である．また，(4.12) より，ウェイト m の固有空間上の 1 次元射影 $|v_m\rangle\langle v_m|$ の $d_{\boldsymbol{\lambda}}$ 倍で T が与えられる場合について (4.17) を示せば十分である．ここで，[37] の (5.35) で定義される U_ζ を用いると，

$$\langle \boldsymbol{\lambda}; \boldsymbol{\lambda} | M_{d_{\boldsymbol{\lambda}} |v_m\rangle\langle v_m|}(d\hat{\zeta}) | \boldsymbol{\lambda}; \boldsymbol{\lambda} \rangle = d_{\boldsymbol{\lambda}} |\langle v_m | U_{-\hat{\zeta}} | \boldsymbol{\lambda}; \boldsymbol{\lambda} \rangle|^2 \mu_\Theta(d\hat{\zeta})$$
$$= d_{\boldsymbol{\lambda}} |\langle v_m | \boldsymbol{\lambda} : -\hat{\zeta} \rangle|^2 \mu_\Theta(d\hat{\zeta})$$

と変形できる．μ_0 を単位ベクトルの集合 S 上の不変な測度とし，$x = \|\zeta\|^2$ とし，適当な関数 $p(x)$ を選ぶと，積分 $\mu_\Theta(d\zeta)$ は $\mu_0(d\zeta_0)p(x)dx$ に変形できる．ここで，μ_0 の全積分は 1 となるように選ぶとする．

また，任意の実数 $c \in [0, 1]$ を固定すると，$\{\rho_{\sqrt{c}\zeta_0}\}_\zeta$ は不変部分群 H_1 の作用に関して閉じているため，$\phi(x) := |\langle \boldsymbol{\lambda} : \sqrt{x_{c,\zeta_0}}\zeta_0 | \boldsymbol{\lambda}; \boldsymbol{\lambda} \rangle|^2 = c$ を満たす $a_c > 0$ は ζ_0 に依存せずに定まる．

ゆえに，題意を示すには，不等式

$$\int_0^{x_c} \int_S d_{\boldsymbol{\lambda}} |\langle \boldsymbol{\lambda}; \boldsymbol{\lambda} | \boldsymbol{\lambda} : \sqrt{x}\zeta_0 \rangle|^2 \mu_0(d\zeta_0) p(x) dx = \int_0^{x_c} d_{\boldsymbol{\lambda}} \phi(x) p(x) dx$$
$$\geq \int_0^{x_c} \int_S d_{\boldsymbol{\lambda}} |\langle v_m | \boldsymbol{\lambda} : \sqrt{x}\zeta_0 \rangle|^2 \mu_0(d\zeta_0) p(x) dx$$

を示せば十分である．

$h(x) := \frac{\int_S |\langle v_m|\boldsymbol{\lambda}:\sqrt{x}\zeta_0\rangle|^2\mu_0(d\zeta_0)}{\int_S |\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|\boldsymbol{\lambda}:\sqrt{x}\zeta_0\rangle|^2\mu_0(d\zeta_0)} = \frac{\int_S |\langle v_m|\boldsymbol{\lambda}:\sqrt{x}\zeta_0\rangle|^2\mu_0(d\zeta_0)}{\phi(x)}$ を用いると,

$$\int_0^{x_c}\int_S d_{\boldsymbol{\lambda}}|\langle v_m|\boldsymbol{\lambda},\sqrt{x}\zeta_0\rangle|^2\mu_0(d\zeta_0)p(x)dx = \int_0^{x_c} d_{\boldsymbol{\lambda}}h(x)\phi(x)p(x)dx$$

を得る．$|\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|\boldsymbol{\lambda}:\sqrt{x}\zeta_0\rangle|^2 = \phi(x)$ であるので，適切に n_0 を選ぶと,

$$\begin{aligned} h(x) &= \int_S \frac{|\langle v_m|\boldsymbol{\lambda}:\sqrt{x}\zeta_0\rangle|^2}{|\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|\boldsymbol{\lambda}:\sqrt{x}\zeta_0\rangle|^2}\mu_0(d\zeta_0) \\ &= \int_S \left|\langle v_m|\sum_{n=0}^{\infty}\frac{(\sqrt{x}\sum_{\alpha\in\Phi_{\boldsymbol{\lambda}}^+}\zeta_{0,\alpha}\mathsf{K}_{-\alpha})^n}{n!}|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\right|^2\mu_0(d\zeta_0) \\ &= x^{n_0}\int_S \left|\langle v_m|\frac{(\sum_{\alpha\in\Phi_{\boldsymbol{\lambda}}^+}\zeta_{0,\alpha}\mathsf{K}_{-\alpha})^{n_0}}{n_0!}|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\right|^2\mu_0(d\zeta_0) \end{aligned}$$

が成り立つことから，$h(x)$ は x に関して単調増加となる．ここで，$\Phi_{\boldsymbol{\lambda}}^+$ は正のルートの集合 Φ^+ の部分集合 $\{\boldsymbol{\alpha}\in\Phi^+\,|\,(\boldsymbol{\alpha},\boldsymbol{\lambda})>0\}$ として定義した．したがって，定理 4.1.4 の証明と同様にして題意を示すことができる． □

4.2 近似状態の生成

4.2.1 近似状態生成の一般論

本節では，群 G の 2 つの空間 $\mathcal{H}$, $\mathcal{H}_1$ 上の状態族 ρ_θ, $\rho_{1,\theta}$ に注目する．そして，系 $\mathcal{H}$ 上の POVM $M=\{M_\omega\}$ を用いて測定し，測定値 ω に応じて，状態 ρ_ω を準備し，状態 ρ_ω が $\rho_{1,\theta}$ に近くなるようにする．この操作を $\hat{M} := (M, \{\rho_\omega\})$ で記述し，**近似状態の生成**または measurement and state preparation (MSP) とよぶことにする [99].

一般に，真の状態 $\rho_{1,\theta}$ に対する近似状態 ρ_ω による近似の誤差を測る関数 $f(\rho_{1,\theta},\rho_\omega)$ が与えられたとき，操作 $\hat{M}$ の性能は $\mathcal{D}_{f,\theta}(\hat{M}) := \int_\Omega f(\rho_{1,\theta},\rho_\omega)$ $\mathrm{Tr}\,\rho_\theta M_\omega d\omega$ で評価できる．この値についても，前節の議論と同じように，$\mathcal{D}_f(\hat{M}) := \max_{\theta\in\Theta}\mathcal{D}_{f,\theta}(\hat{M})$ および $\mathcal{D}_{f,\nu}(\hat{M}) := \int_\Theta \mathcal{D}_{f,\theta}(\hat{M})\nu(d\theta)$ を考えることができる．本節ではこれらの量の最小化を扱う．

以下，2 つの空間 $\mathcal{H}$, $\mathcal{H}_1$ に対して，連結 Lie 群 G のユニタリ表現 f, f_1 が与えられ，ρ_θ, $\rho_{1,\theta}$ が $\Theta = G/H$ をパラメータ空間とする 2 つの表現 f, f_1 に関

する共変的状態族となる場合を考える．Lie 群 G はコンパクトであるか，もしくは条件 (4.14) を満たすとする．このとき，MSP $\hat{M} := (M, \{\rho_\omega\})$ が以下の条件を満たすとき，共変的という．

(1) M は G に値を持つ共変的 POVM である．

(2) $M_{g\omega} = \mathsf{f}(g)M_\omega\mathsf{f}(g)^\dagger$ となる $\omega, g \in G$ に対して，$\rho_{1,g\omega} = \mathsf{f}_1(g)\rho_{1,\omega}\mathsf{f}_1(g)^\dagger$ が成り立つ．

そして，共変的 MSP は $\mathcal{H}$ 上の状態 ρ と $\mathcal{H}_1$ 上の状態 ρ_1 を用いて，以下のように与えられる．

$$M(dg) = d_\lambda \mathsf{f}(g)\rho\mathsf{f}(g)^\dagger \mu_G(dg), \quad \rho_{1,g} = \mathsf{f}_1(g)\rho_1\mathsf{f}_1(g)^\dagger.$$

以下ではこの共変的 MSP を $\hat{M}_{\rho,\rho_1}$ と記すことにする．測定値集合が G ではなく，その等質空間である場合も，測定値集合が G である場合の特殊例として扱うことができる．以下の議論では，近似の誤差を測る関数 $f(\rho_{1,\theta}, \rho_\omega)$ が以下の表現 f の下での不変性を満たす場合を考える．

$$f(\rho_{1,\theta}, \rho_\omega) = f(\mathsf{f}(g)\rho_{1,\theta}\mathsf{f}(g)^\dagger, \mathsf{f}(g)\rho_\omega\mathsf{f}(g)^\dagger), \quad \forall g \in G. \tag{4.19}$$

そして，先の節の議論と同じように，Lie 群 G がコンパクトの場合は，不変測度 μ_Θ を考えることができる．そのため定理 4.1.1 と似た以下の定理が成り立つ．

定理 4.2.1　Lie 群 G がコンパクトであり，近似の誤差を測る関数 f が (4.19) を満たすとき，

$$\min_{\hat{M}} \mathcal{D}_f(\hat{M}) = \min_{\rho,\rho_1} \mathcal{D}_f(\hat{M}_{\rho,\rho_1}) = \min_{\hat{M}} \mathcal{D}_{f,\mu_\Theta}(\hat{M}) = \min_{\rho,\rho_1} \mathcal{D}_{f,\mu_\Theta}(\hat{M}_{\rho,\rho_1})$$

が成り立つ．また，非コンパクトの場合でも第1式は成り立つ．

証明.　確率分布 $\nu(d\omega)$ を用いて，POVM M が $M_\omega \nu(d\omega)$ と記述できるとする．このとき，

$$\begin{aligned}
\int_G \mathcal{D}_{f,g\theta_0}(\hat{M})\mu(dg) &= \int_G \int_\Omega f(\rho_{1,g\theta_0}, \rho_\omega) \operatorname{Tr} \rho_{g\theta} M_\omega \nu(d\omega)\mu(dg) \\
&= \int_G \int_\Omega f(\rho_{1,\theta_0}, \mathsf{f}_1(g)^\dagger \rho_\omega \mathsf{f}_1(g)) \operatorname{Tr} \rho_\theta \mathsf{f}(g)^\dagger M_\omega \mathsf{f}(g)\nu(d\omega)\mu(dg)
\end{aligned}$$

$$= \int_\Omega \frac{\mathrm{Tr}\, M_\omega}{d_\lambda} d_\lambda \int_G f(\rho_{1,\theta_0}, \mathsf{f}_1(g)^\dagger \rho_\omega \mathsf{f}_1(g)) \,\mathrm{Tr}\, \rho_\theta \mathsf{f}(g)^\dagger \frac{M_\omega}{\mathrm{Tr}\, M_\omega} \mathsf{f}(g) \mu(dg) \nu(d\omega)$$

$$= \int_\Omega \mathcal{D}_f \left(\hat{M}_{\frac{M_\omega}{\mathrm{Tr}\, M_\omega}, \rho_\omega} \right) \frac{\mathrm{Tr}\, M_\omega}{d_\lambda} \nu(d\omega).$$

$\frac{\mathrm{Tr}\, M_\omega}{d_\lambda}\nu(d\omega)$ は Ω 上の確率分布を与えることから，

$$\min_{\hat{M}} \mathcal{D}_{f,\mu_\Theta}(\hat{M}) \ge \min_{\rho,\rho_1} \mathcal{D}_{f,\mu_\Theta}(\hat{M}_{\rho,\rho_1}) = \min_{\rho,\rho_1} \mathcal{D}_f(\hat{M}_{\rho,\rho_1})$$

を得る．逆方向の不等式，

$$\min_{\rho,\rho_1} \mathcal{D}_f(\hat{M}_{\rho,\rho_1}) \ge \min_{\hat{M}} \mathcal{D}_f(\hat{M}) \ge \min_{\hat{M}} \mathcal{D}_{f,\mu_\Theta}(\hat{M})$$

が成り立つことから題意を得る． □

4.2.2 擬忠実度の下での近似状態生成の一般論

しかし，一般の近似誤差を与える関数 $f(\rho_{1,g\theta_0}, \rho_\omega)$ の扱いは容易ではない．以下では，擬忠実度 $F(\rho_{1,g\theta_0}, \rho_\omega) = \mathrm{Tr}\, \rho_{1,g\theta_0}\rho_\omega$ の平均値を最大化する場合を扱う．

定理 4.2.2 Lie 群 G の表現空間 $\mathcal{U}_{\boldsymbol{\lambda}} \otimes \mathcal{U}_{\boldsymbol{\lambda}_1}$ に含まれる任意の既約な表現空間 $\mathcal{H}$ と ρ_{θ_0}, ρ_{1,θ_0} に対して，$c(\mathcal{H}) := \frac{\mathrm{Tr}\, P(\mathcal{H})\rho_{\theta_0} \otimes \rho_{1,\theta_0}}{\dim \mathcal{H}}$ を定義する．ここで，$P(\mathcal{H})$ を $\mathcal{H}$ への射影とする．$\mathcal{U}_{\boldsymbol{\lambda}} \otimes \mathcal{U}_{\boldsymbol{\lambda}_1}$ の中で最も大きな最高ウェイトを持つ表現空間 $\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}$（重複度は 1 であるため一意に定まる）が

$$c_0 := c(\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}) \ge c(\mathcal{H}) \tag{4.20}$$

を満たすとする．このとき，

$$\max_{\rho,\rho_1} \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \mathcal{D}_F(\hat{M}_{|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|, |\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1\rangle\langle\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1|}) = d_{\boldsymbol{\lambda}} c_0$$

が成り立つ．すなわち，最適測定は $|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|$ が生成する共変的測定であり，$|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|$ に対応する測定値を得たときに，$|\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1\rangle\langle\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1|$ と推測する方法が最適となる．

なお，G が非コンパクト群のときは，$\dim \mathcal{H}$, $d_{\boldsymbol{\lambda}}$ は形式的次元とする．

証明.　ρ と ρ_1 を用いて，特徴付けられる MSP を用いた場合，$\mathcal{D}_{F,\theta}(\hat{M})$ は以下のように計算できる．

$$
\begin{aligned}
&\mathcal{D}_{F,\theta_0}(\hat{M}_{\rho,\rho_1})\\
&= \int_G (\mathrm{Tr}_{\mathcal{H}_1}\, \rho_{1,\theta_0} \mathsf{f}_{\boldsymbol{\lambda}_1}(g)\rho_1 \mathsf{f}_{\boldsymbol{\lambda}_1}(g)^\dagger)(\mathrm{Tr}_{\mathcal{H}}\, \rho_{\theta_0} d_{\boldsymbol{\lambda}} \mathsf{f}_{\boldsymbol{\lambda}}(g)\rho \mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger)\mu_G(dg)\\
&= d_{\boldsymbol{\lambda}} \int_G \mathrm{Tr}_{\mathcal{H}_1\otimes\mathcal{H}}(\rho_{1,\theta_0}\otimes\rho_{\theta_0})(\mathsf{f}_{\boldsymbol{\lambda}_1}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g))(\rho_1\otimes\rho)(\mathsf{f}_{\boldsymbol{\lambda}_1}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g))^\dagger \mu_G(dg)\\
&= d_{\boldsymbol{\lambda}}\, \mathrm{Tr}_{\mathcal{H}_1\otimes\mathcal{H}} \left[\int_G (\mathsf{f}_{\boldsymbol{\lambda}_1}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g))^\dagger(\rho_{1,\theta_0}\otimes\rho_{\theta_0})(\mathsf{f}_{\boldsymbol{\lambda}_1}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g))\mu_G(dg)\right](\rho_1\otimes\rho).
\end{aligned}
$$

Schur の補題より，$[\int_G (\mathsf{f}_{\boldsymbol{\lambda}_1}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g))^\dagger(\rho_{1,\theta_0}\otimes\rho_{\theta_0})(\mathsf{f}_{\boldsymbol{\lambda}_1}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g))\mu_G(dg)]$ は適切に既約な部分空間 $\mathcal{H}_1,\ldots,\mathcal{H}_k$ を選ぶことにより，$\sum_{j=1}^k c(\mathcal{H}_j)P(\mathcal{H}_j)$ と書ける．したがって，条件 (4.20) より，$d_{\boldsymbol{\lambda}}\,\mathrm{Tr}_{\mathcal{H}_1\otimes\mathcal{H}} \sum_{j=1}^k c(\mathcal{H}_j)P(\mathcal{H}_j)(\rho_1\otimes\rho)$ は $\rho_1\otimes\rho$ が $\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}$ に含まれる密度行列のときに最大値 $d_{\boldsymbol{\lambda}} c(\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1})$ をとる．例えば，$\rho_1\otimes\rho$ が $|\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1\rangle\langle\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1|\otimes|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}| = |\boldsymbol{\lambda}_1+\boldsymbol{\lambda};\boldsymbol{\lambda}_1+\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda}_1+\boldsymbol{\lambda};\boldsymbol{\lambda}_1+\boldsymbol{\lambda}|$ となるとき，最大値 $d_{\boldsymbol{\lambda}} c(\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1})$ が実現される．　□

条件 (4.20) について以下の補題が成り立つ

補題 4.2.3　2つの群 $G'\subset G$ が存在し，G の表現 f, f_1 の部分表現として，G' の表現が与えられて，G' について条件 (4.20) が成り立つとする．そして，G' についての最も大きな最高ウェイトを持つ表現空間 $\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}$ が，G の表現についても閉じているとする．このとき，G について条件 (4.20) が成り立つ．

なお，状態近似の問題は，前節で扱った状態推定の問題と，密接な関係がある．一方で，状態推定では誤差関数のとり方に，様々な選択肢があるので，一般の誤差関数の場合の状態推定と状態近似との間には関係はない．しかし，誤差関数として，$1-F(\rho_{1,\theta},\rho_\omega)$ を用いる場合，以下のような関係がある．状態近似では，推測値として，Θ 以外の値を答えることができる．したがって，ある測定が状態測定の範囲で最適な測定であっても，状態近似まで範囲を広げると，必ずしも最適とは限らない．上記の定理 4.2.2 は，状態近似まで範囲を広げても，測定 $\hat{M}_{|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|,|\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1\rangle\langle\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1|}$ が最適であることを示している．

ここで与えた最適な測定は測定値を連続値に持つ．そのため，その実現が困

難となり，離散値の測定で最適な性能が実現できるか興味のあるところである．この問題を扱うために Θ 上の測度 ν が

$$d_{\boldsymbol{\lambda}} \int_{\Theta} |\boldsymbol{\lambda} : \theta\rangle\langle\boldsymbol{\lambda} : \theta| \nu(d\theta) = I_{\boldsymbol{\lambda}} \tag{4.21}$$

を満たすとき，ν を $\boldsymbol{\lambda}$-design とよぶことにする．（無限次元表現の場合は，形式的次元が存在すると仮定する．）さらに，

$$\left\| d_{\boldsymbol{\lambda}} \int_{\Theta'} |\boldsymbol{\lambda} : \theta\rangle\langle\boldsymbol{\lambda} : \theta| \nu(d\theta) - I_{\boldsymbol{\lambda}} \right\| \le \epsilon \tag{4.22}$$

を満たすとき，作用素ノルム ϵ $\boldsymbol{\lambda}$-design 測度とよぶ．これらについて詳しくは [37, 4.5.2 項] を参照のこと．これらについて以下の定理が成り立つ．

定理 4.2.4　$\mathcal{H}_1 = \mathcal{U}_{\boldsymbol{\lambda}_1}$ $\mathcal{H} = \mathcal{U}_{\boldsymbol{\lambda}}$ とする．$\boldsymbol{\lambda}$-design 測度 ν について測定 $M_\nu(d\hat{\theta}) := d_{\boldsymbol{\lambda}}|\boldsymbol{\lambda} : \hat{\theta}\rangle\langle\boldsymbol{\lambda} : \hat{\theta}|\nu(d\hat{\theta})$ が定義できる．そして，ν が $\boldsymbol{\lambda} + \boldsymbol{\lambda}_1$-design 測度であるとき，$\hat{M}_\nu$ を測定 M_ν を行い，測定値 $\hat{\theta}$ に対して，状態 $|\boldsymbol{\lambda}_1 : \hat{\theta}\rangle\langle\boldsymbol{\lambda}_1 : \hat{\theta}|$ を準備する状態近似とすると，$\mathcal{D}_{F,\theta}(\hat{M}_\nu) = d_{\boldsymbol{\lambda}} c_0$ が成り立つ．特に，条件 (4.20) が成り立つとき，この測定が最適な MSP を与える．

証明.　定理 4.2.2 の最初の式と同じようにして，以下の式の第 1 等式が得られる．

$$\begin{aligned}\mathcal{D}_{F,\theta}(\hat{M}_\nu) &= \operatorname{Tr} \rho_{1,\theta_0} \otimes \rho_{\theta_0} \int_{\Theta'} d_{\boldsymbol{\lambda}} |\boldsymbol{\lambda} + \boldsymbol{\lambda}_1 : \hat{\theta}\rangle\langle\boldsymbol{\lambda} + \boldsymbol{\lambda}_1 : \hat{\theta}| \nu(d\hat{\theta}) \\ &= \operatorname{Tr} \rho_{1,\theta_0} \otimes \rho_{\theta_0} I_{\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}} \frac{d_{\boldsymbol{\lambda}}}{d_{\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}}} = d_{\boldsymbol{\lambda}} c_0.\end{aligned}$$

□

Θ 上の作用素ノルム ϵ $\boldsymbol{\lambda}$-design 測度 p について，$Y_{\boldsymbol{\lambda},p} := \int_\Theta d_{\boldsymbol{\lambda}} |\boldsymbol{\lambda} : \hat{\theta}\rangle\langle\boldsymbol{\lambda} : \hat{\theta}| p(d\hat{\theta})$ を用いて，POVM $M_p(d\hat{\theta}) := Y_{\boldsymbol{\lambda},p}^{-1/2} d_{\boldsymbol{\lambda}} |\boldsymbol{\lambda} : \hat{\theta}\rangle\langle\boldsymbol{\lambda} : \hat{\theta}| Y_{\boldsymbol{\lambda},p}^{-1/2}$ を定義すると，以下の定理が成り立つ．

定理 4.2.5　p が作用素ノルム ϵ $\boldsymbol{\lambda}$-design 測度であり，かつ，作用素ノルム ϵ_1 $\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}$-design 測度 p については定理 4.2.4 と同じように，M_p から $\hat{M}_p$ を定義すると，$|\mathcal{D}_{F,\theta}(\hat{M}_p) - d_{\boldsymbol{\lambda}} c_0| \le (\epsilon_1 + 2\epsilon) d_{\boldsymbol{\lambda}} c_0$ が成り立つ．

証明.　定理 4.2.2 の証明と同じように,

$$\mathcal{D}_{F,\theta}(\hat{M}_p) = \frac{d_{\boldsymbol{\lambda}}}{d_{\boldsymbol{\lambda}_1+\boldsymbol{\lambda}}} \operatorname{Tr} \rho_{1,\theta_0} \otimes \rho_{\theta_0} I \otimes Y_{\boldsymbol{\lambda},p}^{-1/2} Y_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1,p} I \otimes Y_{\boldsymbol{\lambda},p}^{-1/2}$$

が示せる. $(1-(\epsilon+\epsilon_1))I \le I \otimes Y_{\boldsymbol{\lambda},p}^{-1/2} Y_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1,p} I \otimes Y_{\boldsymbol{\lambda},p}^{-1/2} \le (1+(2\epsilon+\epsilon_1))I$ であるので, 題意を得る. □

4.2.3　純粋状態の近似状態生成

次に, 状態族 ρ_{θ_0}, ρ_{1,θ_0} がともに, 以下のようにコヒーレント状態族である場合を考えよう.

$$\rho_{\theta_0} = \mathsf{f}_{\boldsymbol{\lambda}}(g(\theta))|\boldsymbol{\lambda};\boldsymbol{\lambda}\rangle\langle\boldsymbol{\lambda};\boldsymbol{\lambda}|\mathsf{f}_{\boldsymbol{\lambda}}(g(\theta))^\dagger$$

$$\rho_{1,\theta_0} = \mathsf{f}_{\boldsymbol{\lambda}_1}(g(\theta))|\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1\rangle\langle\boldsymbol{\lambda}_1;\boldsymbol{\lambda}_1|\mathsf{f}_{\boldsymbol{\lambda}_1}(g(\theta))^\dagger.$$

この設定は Boson のコヒーレント状態の場合も含む. この場合, 擬忠実度は, 忠実度に一致するため, 以下の議論は基準として忠実度を用いたと考えることができる. そして, $c(\mathcal{H})$ は $\mathcal{H}$ が $\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}$ と異なる場合は, 0 となり, $\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}$ の場合は $1/d_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}$ となり条件 (4.20) を満たす. よって,

$$\max_{\hat{M}} \mathcal{D}_F(\hat{M}) = \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \frac{d_{\boldsymbol{\lambda}}}{d_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}} \tag{4.23}$$

が成り立つ.

一般には, $\operatorname{Tr} \rho_\theta \rho_{\hat{\theta}}$ で精度を評価する状態推定と近似状態の生成を比較すると, 近似状態の生成の方が広い選択肢を持つので, 近似状態の生成の方が精度が良くなる. しかし, この例では, 最適な近似状態の生成での推測値として与える状態は候補となる状態族 $\{\rho_\theta\}$ に含まれる. そのため, 両者の精度は等しくなる.

例 4.2.6　($\boldsymbol{\lambda} = n\boldsymbol{\lambda}_1$ の場合)　4.1 節で述べたように, $\boldsymbol{\lambda} = n\boldsymbol{\lambda}_1$ となる場合について考えよう. このときの精度は $\max_{\hat{M}} \mathcal{D}_F(\hat{M}) = \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \frac{d_{n\boldsymbol{\lambda}_1}}{d_{(n+1)\boldsymbol{\lambda}_1}}$ となる.

$\mathfrak{g} = \mathfrak{su}(2), \mathfrak{su}(1,1)$ の場合は, λ_1 は $\lambda_1 < 0$ の実数か, 正の半整数となる. そして, 精度は $\frac{d_{n\lambda_1}}{d_{(n+1)\lambda_1}} = \frac{2n\lambda+1}{2(n+1)\lambda+1} = 1 - \frac{1}{n+1+\frac{1}{2\lambda}} \cong 1 - \frac{1}{n} + (1+\frac{1}{2\lambda})\frac{1}{n^2}$ となる.

$\mathfrak{g} = \mathfrak{h}(2,\mathbb{R}) \rtimes \mathfrak{u}(1)$ の場合は $\boldsymbol{\lambda}_1 = (\lambda_Z, \lambda_F)$ となる．そして，精度は $\frac{d_{n\boldsymbol{\lambda}_1}}{d_{(n+1)\boldsymbol{\lambda}_1}} = \frac{n\lambda_Z}{(n+1)\lambda_Z} = 1 - \frac{1}{(n+1)} \cong 1 - \frac{1}{n} + \frac{1}{n^2}$ となる．

$\mathfrak{g} = \mathfrak{su}(r)$ の場合で $\boldsymbol{\lambda}_1 = [1, 0, \ldots, 0]$ のときを考えよう．精度は $\frac{d_{n\boldsymbol{\lambda}_1}}{d_{(n+1)\boldsymbol{\lambda}_1}} = \frac{n+1}{n+1+r-1} = 1 - \frac{r-1}{n+r} \cong 1 - \frac{r-1}{n} + r(r-1)\frac{1}{n^2}$ となる．

$\mathfrak{g} = \mathfrak{h}(2r,\mathbb{R}) \rtimes \mathfrak{u}(r)$ の場合は $\boldsymbol{\lambda}_1 = (\lambda_Z, \lambda_F \boldsymbol{v})$ となる．そして，精度は $\frac{d_{n\boldsymbol{\lambda}_1}}{d_{(n+1)\boldsymbol{\lambda}_1}} = \frac{n^r \lambda_Z^r}{(n+1)^r \lambda_Z^r} = (1 - \frac{1}{(n+1)})^r \cong 1 - \frac{r}{n} + \frac{r(r+1)}{2}\frac{1}{n^2}$ となる．

例 4.2.7 （群 $\mathrm{H}(2,\mathbb{R}) \times \mathrm{U}(1)$ の下での 1 モードのスクイズド状態 [94]） 表現 f, f_1 が群 $G = \mathrm{H}(2,\mathbb{R}) \times \mathrm{U}(1)$ の $L^2(\mathbb{R}) = \mathcal{U}_{1,0}$ への Heisenberg 表現（詳しくは [37] の 6.1 節を参照．）として与えられ，パラメータ空間 Θ が G と等しく，ρ_{θ_0}, ρ_{1,θ_0} がともに，スクイズド状態 $|\zeta,\zeta'\rangle\langle\zeta,\zeta'|$ で与えられている場合を考えよう．（ここで，ζ は sift に関するパラメータで，ζ' はスクイジングに関するパラメータである．詳しくは，[37] の 6.5 節を参照．）G の作用を考えることにより，ρ_{θ_0}, ρ_{1,θ_0} が $|\zeta,0\rangle\langle\zeta,0|$ であるとして一般性を失わない．そして，最高ウェイトが $-n$ となる空間への射影は [37] の 6.3 節で与えた作用素 $\mathsf{U}_{1,2}$ を用いると，$\mathsf{U}_{1,2}^\dagger (I \otimes |n\rangle\langle n|) \mathsf{U}_{1,2}$ で与えられる．

$|\zeta,0\rangle \otimes |\zeta,0\rangle$ は $L^2(\mathbb{R}) \otimes L^2(\mathbb{R})$ への群 $\mathrm{SU}(1,1)$ のテンソル積表現についてのコヒーレントベクトルとなり，その最高ウェイトは $\lambda = -1/2$ となる．この表現では $\mathsf{K}_{-,-1} = \frac{1}{2}((\mathsf{a}_1^\dagger)^2 + (\mathsf{a}_2^\dagger)^2) = \mathsf{U}(g_0)^\dagger \frac{1}{2}((\mathsf{a}_1^\dagger)^2 + (\mathsf{a}_2^\dagger)^2)\mathsf{U}(g_0)$ となる．

$$
\begin{aligned}
|\zeta,0\rangle \otimes |\zeta,0\rangle &= (1 - |\zeta|^2)^{1/2} \exp(\zeta((\mathsf{a}_1^\dagger)^2 + (\mathsf{a}_2^\dagger)^2))|0,0\rangle \\
&= \mathsf{U}(g_0)^\dagger (1 - |\zeta|^2)^{1/2} \exp(\zeta((\mathsf{a}_1^\dagger)^2 + (\mathsf{a}_2^\dagger)^2))\mathsf{U}(g_0)|0,0\rangle \\
&= \mathsf{U}(g_0)^\dagger (1 - |\zeta|^2)^{1/2} \exp(\zeta((\mathsf{a}_1^\dagger)^2 + (\mathsf{a}_2^\dagger)^2))|0,0\rangle = \mathsf{U}(g_0)^\dagger |\zeta,0\rangle \otimes |\zeta,0\rangle
\end{aligned}
$$

が成り立つので，

$$
\begin{aligned}
&\mathrm{Tr}\, \mathsf{U}(g_0)^\dagger (I \otimes |n\rangle\langle n|) \mathsf{U}(g_0) |\zeta,0\rangle\langle\zeta,0| \otimes |\zeta,0\rangle\langle\zeta,0| \\
&= \mathrm{Tr}\, \mathsf{U}(g_0)^\dagger (I \otimes |n\rangle\langle n|) \mathsf{U}(g_0) \mathsf{U}(g_0)^\dagger |\zeta,0\rangle\langle\zeta,0| \otimes |\zeta,0\rangle\langle\zeta,0| \mathsf{U}(g_0)^\dagger \\
&= \mathrm{Tr}(I \otimes |n\rangle\langle n|) |\zeta,0\rangle\langle\zeta,0| \otimes |\zeta,0\rangle\langle\zeta,0| = |\langle n|\zeta,0\rangle|^2
\end{aligned}
$$

を得る．n が奇数のときは 0 となり，n が偶数のときは，

$$|\langle 2n|\zeta,0\rangle|^2 = \left|(1-|\zeta|^2)^{1/4}\langle 2n|\frac{\zeta^n(\mathsf{a}_2^\dagger)^{2n}}{2^n n!}|0\rangle\right|^2 = (1-|\zeta|^2)^{1/2}\frac{|\zeta|^{2n}(2n)!}{(2^n n!)^2}$$

となる．$|\zeta|^2<1$ であり，$\frac{(2n)!}{(2^n n!)^2}$ は n について単調減少であるので，$n=0$ のとき最大値 $(1-|\zeta|^2)^{1/2}$ をとる．よって条件 (4.20) が成り立つ．テンソル積空間内の G の既約表現の形式的次元は 2 であるので，$c_0=(1-|\zeta|^2)^{1/2}/2$ となり，

$$\max_{\hat{M}}\mathcal{D}_F(\hat{M}) = \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \frac{(1-|\zeta|^2)^{1/2}}{2}$$

を得る．

例 4.2.8（群 $\mathrm{H}(2r,\mathbb{R})\times\mathrm{U}(r)$ の下での r モードのスクイズド状態*）　表現 f, f_1 が群 $G=\mathrm{H}(2r,\mathbb{R})\times\mathrm{U}(r)$ の $L^2(\mathbb{R})^{\otimes r}$ への表現として与えられ，パラメータ空間 Θ が G と等しく，ρ_{θ_0}，ρ_{1,θ_0} がともに，r モードのスクイズド状態 $|\frac{-1}{2}\boldsymbol{v},\zeta\rangle\langle\frac{-1}{2}\boldsymbol{v},\zeta|$ で与えられている場合を考えよう．($|\frac{-1}{2}\boldsymbol{v},\zeta\rangle\langle\frac{-1}{2}\boldsymbol{v},\zeta|$ の定義については [37] の 6.1 節を参照．) 複素対称行列 ζ に対して適切なユニタリ行列 g を選ぶことで，$g\zeta g^T$ は対角成分を $\zeta_1,\ldots,\zeta_r$ とする対角行列となる．したがって，$|\frac{-1}{2}\boldsymbol{v},\zeta\rangle = |\zeta_1,0\rangle\otimes\cdots\otimes|\zeta_r,0\rangle$ として一般性を失わない．

以下，G' が $\mathrm{H}(2r,\mathbb{R})\times\mathrm{U}(1)^r$ で与えられる場合について，補題 4.2.3 の適用を検討する．ここで，$\mathrm{U}(1)^r$ は各モードに $\mathrm{U}(1)$ の要素を個別に作用させる群とする．すなわち，$\mathrm{U}(r)$ の対角な要素からなる群である．このとき，先の例の議論より，G' について条件 (4.20) が成り立つ．$\mathrm{H}(2r,\mathbb{R})$ の作用に関して既約な空間は，$\mathrm{H}(2r,\mathbb{R})\times\mathrm{U}(r)$ の作用に関しても既約であるので，補題 4.2.3 が適用でき，$\mathrm{H}(2r,\mathbb{R})\times\mathrm{U}(r)$ についても，条件 (4.20) が成り立つ．したがって，

$$\max_{\hat{M}}\mathcal{D}_F(\hat{M}) = \max_{\rho,\rho_1}\mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \prod_{j=1}^{r}\frac{(1-|\zeta_j|^2)^{1/2}}{2} = \sqrt{\det\frac{I-\overline{\zeta}\zeta}{2}}$$

を得る．特に右辺は $\mathrm{U}(r)$ の作用に関して不変な量であるので，

$$\max_{\hat{M}}\mathcal{D}_F(\hat{M}) = \max_{\rho,\rho_1}\mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \sqrt{\det\frac{I-\overline{\zeta}\zeta}{2}}$$

は任意の r モードのスクイズド状態について成り立つ．

4.2.4 混合状態の近似状態生成：擬忠実度

以下では，G が Lie 群であり，状態 ρ_0 および，$\rho_{1,0}$ がその Lie 環 $\mathfrak{g}$ の極大カルタン部分代数の要素 X と定数 $c, c_1 > 0$ を用いて，$ce^{i\mathsf{f}(X)}$ および $c_1 e^{i\mathsf{f}_1(X)}$ で与えられる場合に擬忠実度を基準にして近似状態生成を扱う．すなわち，状態族は

$$\rho_\theta := c\mathsf{f}(g(\theta))e^{i\mathsf{f}(X)}\mathsf{f}(g(\theta))^\dagger,\ \rho_{1,\theta} := c_1\mathsf{f}_1(g(\theta))e^{i\mathsf{f}_1(X)}\mathsf{f}_1(g(\theta))^\dagger$$

で与えられる．テンソル積表現 $\mathsf{f}' \otimes \mathsf{f}'_1$ の既約分解が $\mathcal{H} \otimes \mathcal{H}_1 = \bigoplus_{\boldsymbol{\lambda}} \mathcal{U}_{\boldsymbol{\lambda}}$ で与えられるとき，個々の表現空間への表現を $\mathsf{f}_{\boldsymbol{\lambda}}$ とすると，$c(\mathcal{U}_{\boldsymbol{\lambda}}) = cc_1 \frac{\mathrm{Tr}\, e^{i\mathsf{f}_{\boldsymbol{\lambda}}(X)}}{\dim \mathcal{U}_{\boldsymbol{\lambda}}}$ となる．したがって，定理 4.2.2 の条件 (4.20)，すなわち，上記の既約分解に現れる $\boldsymbol{\lambda}$ について $c(\mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}) > c(\mathcal{U}_{\boldsymbol{\lambda}})$ が成り立つとき，

$$\max_{\hat{M}} \mathcal{D}_F(\hat{M}) = \max_{\rho,\rho_1} \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = \dim \mathcal{U}_{\boldsymbol{\lambda}} cc_1 \frac{\mathrm{Tr}\, e^{i\mathsf{f}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}(X)}}{\dim \mathcal{U}_{\boldsymbol{\lambda}+\boldsymbol{\lambda}_1}}$$

が成り立つ．以下，この事実を用いて具体例を調べよう．

例 4.2.9 $\mathfrak{g} = \mathfrak{su}(2)$ であり，$\mathcal{H} = \mathcal{U}_\lambda$, $\mathcal{H}_1 = \mathcal{U}_{\lambda_1}$ とする．そして，$t, c, c_1 > 0$ を用いて，$\rho_0 = ce^{t\mathsf{E}_{0,1}}$, $\rho_{1,0} = c_1 e^{t\mathsf{E}_{0,1}}$ と書けるとする．このとき，$c = \frac{e^t - 1}{e^{t(\lambda+1)} - e^{-t\lambda}}$, $c_1 = \frac{e^t-1}{e^{t(\lambda_1+1)} - e^{-t\lambda_1}}$ となる．そして，$\lambda' > 0$ について，$c(\mathcal{U}_{\lambda'}) = cc_1 \frac{e^{t(\lambda'+1)} - e^{-t\lambda'}}{(e^t-1)(2\lambda'+1)}$ と計算できる．したがって，$\lambda' > \lambda'' > 0$ となる 2 つの λ', λ'' に対して $c(\mathcal{U}_{\lambda'}) > c(\mathcal{U}_{\lambda''})$ となるので，条件 (4.20) が成り立つ．したがって，

$$\begin{aligned}\max_{\hat{M}} \mathcal{D}_F(\hat{M}) &= \max_{\rho,\rho_1} \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = (2\lambda+1)cc_1 \frac{e^{t(\lambda+\lambda_1+1)} - e^{-t(\lambda+\lambda_1)}}{(e^t-1)(2(\lambda+\lambda_1)+1)} \\ &= \frac{(2\lambda+1)(e^t-1)(e^{t(\lambda+\lambda_1+1)} - e^{-t(\lambda+\lambda_1)})}{(2(\lambda+\lambda_1)+1)(e^{t(\lambda_1+1)} - e^{-t\lambda_1})(e^{t(\lambda+1)} - e^{-t\lambda})}\end{aligned}$$

を得る．そして，極限 $t \to \infty$ の下で，純粋状態のときの最適値 $\frac{2\lambda+1}{2(\lambda+\lambda_1)+1}$ と一致する．

例 4.2.10 $\mathfrak{g} = \mathfrak{su}(1,1)$ であり，$\mathcal{H} = \mathcal{U}_\lambda$, $\mathcal{H}_1 = \mathcal{U}_{\lambda_1}$ とする．そして，$t, c, c_1 > 0$ を用いて，$\rho_0 = ce^{t\mathsf{E}_{0,-1}}$, $\rho_{1,0} = c_1 e^{t\mathsf{E}_{0,-1}}$ と書けるとする．このとき，$c = \frac{1-e^{-t}}{e^{t\lambda}}$, $c_1 = \frac{1-e^{-t}}{e^{t\lambda_1}}$ となる．そして，$c(\mathcal{U}_{\lambda'}) = cc_1 \frac{e^{t\lambda'}}{-(2\lambda'+1)(1-e^{-t})}$ と

計算できる．$0 > \lambda' > \lambda''$ に対して $c(\mathcal{U}_{\lambda'}) > c(\mathcal{U}_{\lambda''})$ となるので，条件 (4.20) が成り立つ．したがって，

$$\max_{\hat{M}} \mathcal{D}_F(\hat{M}) = \max_{\rho,\rho_1} \mathcal{D}_F(\hat{M}_{\rho,\rho_1}) = -(2\lambda+1)cc_1 \frac{e^{t(\lambda+\lambda_1)}}{-(2(\lambda+\lambda_1)+1)(1-e^{-t})}$$
$$= \frac{(2\lambda+1)(1-e^{-t})}{2(\lambda+\lambda_1)+1}$$

を得る．そして，極限 $\to \infty$ の下で，純粋状態のときの最適値 $\frac{2\lambda+1}{2(\lambda+\lambda_1)+1}$ と一致する．

例 4.2.11　$\mathfrak{g} = \mathfrak{h}(2,\mathbb{R}) \rtimes \mathfrak{u}(1)$ であり，$\mathcal{H} = \mathcal{U}_{\lambda_Z,\lambda_F}$, $\mathcal{H}_1 = \mathcal{U}_{\lambda_{Z,1},\lambda_{F,1}}$ とする．そして，$t, c, c_1 > 0$ を用いて，$\rho_0 = ce^{-t\mathsf{N}}$, $\rho_{1,0} = c_1 e^{-t\mathsf{N}}$ と書けるとする．このとき，$c = \frac{1-e^{-t}}{e^{t\lambda_F}}$, $c_1 = \frac{1-e^{-t}}{e^{t\lambda_{F,1}}}$ となる．テンソル積空間での形式的次元が 2 であることに注意すると，$c(\mathcal{U}_{\lambda_Z+\lambda_{Z,1},\lambda'_F}) = cc_1 \frac{e^{t\lambda'_F}}{\lambda_Z+\lambda_{Z,1}(1-e^{-t})}$ と計算できる．$\lambda'_F > \lambda''_F$ となる 2 つの整数 λ'_F, λ''_F に対して $c(\mathcal{U}_{\lambda_Z+\lambda_{Z,1},\lambda'_F}) > c(\mathcal{U}_{\lambda_Z+\lambda_{Z,1},\lambda''_F})$ となるので，既約分解（[38] の (6.26) を参照）より，条件 (4.20) が成り立つ．したがって，

$$\max_{\hat{M}} \mathcal{D}_F(\hat{M}) = \max_{\rho,\rho_1} \mathcal{D}_F(\hat{M}_{\rho,\rho_1})$$
$$= \lambda_Z cc_1 \frac{e^{t(\lambda_F+\lambda_{F,1})}}{(\lambda_Z+\lambda_{Z,1})(1-e^{-t})} = \frac{\lambda_Z(1-e^{-t})}{\lambda_Z+\lambda_{Z,1}}$$

を得る．そして，極限 $t \to \infty$ の下で，純粋状態のときの最適値 $\frac{\lambda_Z}{\lambda_Z+\lambda_{Z,1}}$ と一致する．

4.2.5　混合状態の近似状態生成：忠実度

次に，G が Lie 群である場合に，基準を忠実度の二乗にとって，混合状態を近似する状態を生成する問題を考える．しかし，忠実度に基づいた議論は一般には複雑となる．そのため，以下では特殊な場合に限定した議論を行う．

初めに，$\mathfrak{g} = \mathfrak{su}(2)$ であり，$\mathcal{H} = \mathcal{U}_{n/2}$, $\mathcal{H}_1 = \mathcal{U}_{1/2}$ となる場合を考える．定理 4.2.2 より，共変的な MSP に限られることから，$\hat{M}_{\rho,\rho_1}$ に限る．ここで，ρ_1 に対して適切な $g \in \mathrm{SU}(2)$ を選ぶと，$g^\dagger \rho_1 g$ は対角となる．したがって，以下では ρ_1 が対角行列であり，$\rho_{(r',0,0)}$ で与えられる場合を考える．

例 4.2.9 と同じように，$t, c, c_1 > 0$ を用いて，$\rho_0 = ce^{t\mathsf{f}(E_{0,1})}$, $\rho_{1,0} = c_1 e^{tE_{0,1}}$ と書けるとする．そして，$\rho_{1,0} = \rho_{(r,0,0)}$ となるように r を選ぶ．SU(2) を対角行列からなる 1 次元部分群 H で割って得られる等質空間 S^2 に注目し，$T(\rho) := \int_H g\rho g \mu_H(dg)$ を用いると，

$$\begin{aligned}
&\max_{r',\rho} d_{\frac{n}{2}} \int_{\mathrm{SU}(2)} F(\rho_{r,0,0}, \rho_{r',0,0})^2 \operatorname{Tr} ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g)\rho \mathsf{f}_{n/2}(g)^\dagger \mu(dg) \\
&= \max_{r',\rho} d_{\frac{n}{2}} \int_{S^2} F(\rho_{r,0,0}, \rho_{r'\boldsymbol{x}}) \operatorname{Tr} ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g(\boldsymbol{x}))T(\rho)\mathsf{f}_{n/2}(g(\boldsymbol{x}))^\dagger \mu_{S^2}(d\boldsymbol{x})
\end{aligned} \tag{4.24}$$

を得る．ここで，$g(\boldsymbol{x})\rho_{(r,0,0)}g(\boldsymbol{x})^\dagger = \rho_{\boldsymbol{x}}$ を満たすように $g(\boldsymbol{x}) \in \mathrm{SU}(2)$ を選んだ．そして，$\boldsymbol{x}_0 := (1,0,0)$ とすると，(2.44) より，

$$\begin{aligned}
F(\rho_{r,0,0}, \rho_{r'\boldsymbol{x}}) &= \frac{1 + rr'\boldsymbol{x}_0 \cdot \boldsymbol{x} + \sqrt{1-r^2}\sqrt{1-r'^2}}{2} \\
&= r' \frac{1 + r\boldsymbol{x}_0 \cdot \boldsymbol{x}}{2} + \frac{1 - r' + \sqrt{1-r^2}\sqrt{1-r'^2}}{2}
\end{aligned} \tag{4.25}$$

となる．第 1 項のみが確率変数となる．$ce^{t\mathsf{E}_{0,1}} = \rho_{(r,0,0)}$ すなわち $e^t = \frac{1+r}{1-r}$ であることを用いると，その期待値は例 4.2.9 の議論を用いて以下のように評価できる．

$$\begin{aligned}
& d_{\frac{n}{2}} \int_{S^2} \frac{1 + r\boldsymbol{x}_0 \cdot \boldsymbol{x}}{2} \operatorname{Tr} ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g(\boldsymbol{x}))T(\rho)\mathsf{f}_{n/2}(g(\boldsymbol{x}))^\dagger \mu_{S^2}(d\boldsymbol{x}) \\
&= d_{\frac{n}{2}} \int_{S^2} (\operatorname{Tr} \rho_{r,0,0}\rho_{\boldsymbol{x}}) \operatorname{Tr} ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g(\boldsymbol{x}))T(\rho)\mathsf{f}_{n/2}(g(\boldsymbol{x}))^\dagger \mu_{S^2}(d\boldsymbol{x}) \\
&\le \frac{(n+1)(e^t - 1)(e^{(\frac{n+1}{2}+1)t} - e^{-\frac{n+1}{2}t})}{(n+2)(e^{\frac{3}{2}t} - e^{-\frac{1}{2}t})(e^{(\frac{n}{2}+1)t} - e^{-\frac{n}{2}t})} \\
&= \frac{(n+1)((1+r)^{n+2} - (1-r)^{n+2})}{2(n+2)((1+r)^{n+1} - (1-r)^{n+1})}
\end{aligned} \tag{4.26}$$

を得る．$T(\rho)$ が最高ウェイト状態のときに等号を達成する．したがって，(4.25) を用いると，

$$\max_{\rho} d_{\frac{n}{2}} \int_{S^2} F(\rho_{r,0,0}, \rho_{r'\boldsymbol{x}}) \operatorname{Tr} ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g(\boldsymbol{x}))T(\rho)\mathsf{f}_{n/2}(g(\boldsymbol{x}))^\dagger \mu_{S^2}(d\boldsymbol{x})$$

$$= r' \frac{(n+1)((1+r)^{n+2}-(1-r)^{n+2})}{2(n+2)((1+r)^{n+1}-(1-r)^{n+1})} + \frac{1-r'+\sqrt{1-r^2}\sqrt{1-r'^2}}{2}$$

$$= \frac{1}{2} + r' \left(\frac{(n+1)((1+r)^{n+2}-(1-r)^{n+2})}{2(n+2)((1+r)^{n+1}-(1-r)^{n+1})} - \frac{1}{2} \right) + \sqrt{1-r'^2}\frac{\sqrt{1-r^2}}{2} \tag{4.27}$$

$$\leq \frac{1}{2} + \sqrt{\left(\frac{(n+1)((1+r)^{n+2}-(1-r)^{n+2})}{2(n+2)((1+r)^{n+1}-(1-r)^{n+1})} - \frac{1}{2} \right)^2 + \frac{1-r^2}{4}} \tag{4.28}$$

を得る．不等式(4.28)において，適切な r' を選ぶと等号が成り立つことから，(4.24)の最大値は(4.28)の右辺に一致する．

4.2.6　近似状態生成：相対エントロピー

次に，基準を相対エントロピーにとって，混合状態を近似する状態を生成する問題を考える．相対エントロピーに基づいた議論は純粋状態の場合に限っても，忠実度に比べてより複雑な議論が必要となる．この場合，系 $\mathcal{H}$, $\mathcal{H}_1$ 上の状態族 ρ_θ, $\rho_{1,\theta}$ に対して，操作 $\hat{M} = (M, \{\rho_\omega\})$ に対して，$\int_\Theta \int_\Omega D(\rho_{1,\theta} \| \rho_\omega) \operatorname{Tr} \rho_\theta M_\omega d\omega \mu(d\theta)$ を最小化する．ここで状態 $\rho[M]_\omega := \int_\Theta \rho_{1,\theta}(\operatorname{Tr} \rho_\theta M_\omega)\mu(d\theta)$ を用いると，この値は

$$\int_\Theta \int_\Omega D(\rho_{1,\theta} \| \rho_\omega) \operatorname{Tr} \rho_\theta M_\omega d\omega \mu(d\theta)$$
$$= \int_\Theta H(\rho_{1,\theta})\mu(d\theta) - \int_\Omega \operatorname{Tr} \int_\Theta \rho_{1,\theta}(\operatorname{Tr} \rho_\theta M_\omega)\mu(d\theta) \log \rho_\omega d\omega$$
$$= \int_\Theta H(\rho_{1,\theta})\mu(d\theta) + \int_\Omega \operatorname{Tr} \rho[M]_\omega \left[H\left(\frac{\rho[M]_\omega}{\operatorname{Tr} \rho[M]_\omega} \right) + D\left(\frac{\rho[M]_\omega}{\operatorname{Tr} \rho[M]_\omega} \| \rho_\omega \right) \right] d\omega \tag{4.29}$$

と計算できるので，POVM $M = \{M_\omega\}$ を与えたとき，M に対して最適な ρ_ω は $\frac{\rho[M]_\omega}{\operatorname{Tr} \rho[M]_\omega}$ となる．したがって，

$$\int_\Theta H(\rho_{1,\theta})\mu(d\theta) + \int_\Omega \operatorname{Tr} \rho[M]_\omega H\left(\frac{\rho[M]_\omega}{\operatorname{Tr} \rho[M]_\omega} \right) d\omega \tag{4.30}$$

を最小化するPOVM M を求めることが問題となる．ここで，系 $\mathcal{H} \otimes \mathcal{H}_1$ 上の状態 $\int_\Theta \operatorname{Tr} \rho_\theta \otimes \rho_{1,\theta} \nu(d\theta)$ についての $\mathcal{R}$ を参照系とする純粋状態化 $|x\rangle$ を

考える．$\mathcal{D}_F(\rho)$ の表式 (3.25) より，(4.30) の第二項は $\mathcal{D}_F(\mathrm{Tr}_{\mathcal{H}} |x\rangle\langle x|)$ に一致する．

しかし，一般には $\mathcal{D}_F(\mathrm{Tr}_{\mathcal{H}} |x\rangle\langle x|)$ の計算は容易ではない．そのため，以下では特殊な場合に限定した議論を行う．

初めに，$\mathfrak{g} = \mathfrak{su}(2)$ であり，$\mathcal{H} = \mathcal{U}_{n/2}, \mathcal{H}_1 = \mathcal{U}_{1/2}$ となる場合を考える．定理 4.2.2 より，共変的な MSP に限られることから，$\hat{M}_{\rho,\rho_1}$ に限る．ここで，ρ_1 に対して適切な $g \in \mathrm{SU}(2)$ を選ぶと，$g^\dagger \rho_1 g$ は対角となる．以下の議論では，最初に $\{\rho_\omega\}$ に対応する ρ_1 を固定し，POVM M を最適化する．この議論では，最初に最適な POVM が最高ウェイトから生成される共変的 POVM となることを示す．したがって，以下では ρ_1 が対角行列であり，$\rho_{(r',0,0)}$ で与えられる場合を考える．

例 4.2.9 と同じように，$t, c, c_1 > 0$ を用いて，$\rho_0 = ce^{t\mathsf{f}(E_{0,1})}$, $\rho_{1,0} = c_1 e^{tE_{0,1}}$ と書けるとする．そして，$\rho_{1,0} = \rho_{(r,0,0)}$ となるように r を選ぶ．SU(2) を対角行列からなる 1 次元部分群 H で割って得られる等質空間 S^2 に注目し，$T(\rho) := \int_H g\rho g \mu_H(dg)$ を用いると，

$$
\begin{aligned}
&\min_{r',\rho} d_{\frac{n}{2}} \int_{\mathrm{SU}(2)} D(\rho_{r,0,0} \| \rho_{r',0,0}) \,\mathrm{Tr}\, ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g) \rho \mathsf{f}_{n/2}(g)^\dagger \mu(dg) \\
&\quad = \min_{r',\rho} d_{\frac{n}{2}} \int_{S^2} D(\rho_{r,0,0} \| \rho_{r'\boldsymbol{x}}) \,\mathrm{Tr}\, ce^{t\mathsf{f}(E_{0,1})} \mathsf{f}_{n/2}(g(\boldsymbol{x})) T(\rho) \mathsf{f}_{n/2}(g(\boldsymbol{x}))^\dagger \mu_{S^2}(d\boldsymbol{x})
\end{aligned}
$$

を得る．ここで，$g(\boldsymbol{x}) \rho_{(r,0,0)} g(\boldsymbol{x})^\dagger = \rho_{\boldsymbol{x}}$ を満たすように $\mathfrak{g}(\boldsymbol{x}) \in \mathrm{SU}(2)$ を選んだ．(4.30) より，$\boldsymbol{x}_0 := (1,0,0)$ を用いると，

$$
\begin{aligned}
&D(\rho_{r,0,0} \| \rho_{r'\boldsymbol{x}}) \\
&\quad = h\left(\frac{1+r}{2}\right) - \frac{1 + r\boldsymbol{x}_0 \cdot \boldsymbol{x}}{2} \log\left(\frac{1+r'}{2}\right) - \frac{1 - r\boldsymbol{x}_0 \cdot \boldsymbol{x}}{2} \log\left(\frac{1-r'}{2}\right) \\
&\quad = h\left(\frac{1+r}{2}\right) - \log\left(\frac{1-r'}{2}\right) - \frac{1 + r\boldsymbol{x}_0 \cdot \boldsymbol{x}}{2} \log\left(\frac{1+r'}{1-r'}\right)
\end{aligned}
$$

となる．そして，最終項のみが確率変数である．この値の期待値は (4.26) で評価される．(4.26) で等号が成り立つのは，$T(\rho)$ が最高ウェイト状態のときである．

したがって，以下の最適化の議論では POVM M を最高ウェイトから生成

される共変的 POVM に限ることができる．このとき，最適な ρ_1 は (4.29) より，$d_{\frac{n}{2}} \int_\Theta \mathrm{Tr}\, \rho_{1,\theta} \langle \frac{n}{2}; \frac{n}{2} | \rho_\theta | \frac{n}{2}; \frac{n}{2} \rangle \mu(d\theta)$ となる．

ρ_θ，$\rho_{1,\theta}$ がともに コヒーレント状態すなわち，純粋状態とき，この値は Clebsh-Gordan 係数の公式 [37, (4.19)] を用いると，以下のように計算できる．

$$
\begin{aligned}
& d_{\frac{n}{2}} \int_\Theta \mathrm{Tr}\, \rho_{1,\theta} \left\langle \frac{n}{2}; \frac{n}{2} \middle| \rho_\theta \middle| \frac{n}{2}; \frac{n}{2} \right\rangle \mu(d\theta) \\
&\quad = \frac{d_{\frac{n}{2}}}{d_{\frac{n+1}{2}}} \left| \frac{1}{2}; \frac{1}{2} \right\rangle \left\langle \frac{1}{2}; \frac{1}{2} \right| \left\langle \frac{1}{2}, \frac{n}{2}; \frac{1}{2}, \frac{n}{2} \middle| \frac{n+1}{2}; \frac{n+1}{2} \right\rangle \left\langle \frac{n+1}{2}; \frac{n+1}{2} \middle| \frac{1}{2}, \frac{n}{2}; \frac{1}{2}, \frac{n}{2} \right\rangle \\
&\qquad + \frac{d_{\frac{n}{2}}}{d_{\frac{n+1}{2}}} \left| \frac{1}{2}; -\frac{1}{2} \right\rangle \left\langle \frac{1}{2}; -\frac{1}{2} \right| \left\langle \frac{1}{2}, \frac{n}{2}; -\frac{1}{2}, \frac{n}{2} \middle| \frac{n+1}{2}; \frac{n-1}{2} \right\rangle \\
&\qquad \cdot \left\langle \frac{n+1}{2}; \frac{n-1}{2} \middle| \frac{1}{2}, \frac{n}{2}; -\frac{1}{2}, \frac{n}{2} \right\rangle \\
&\quad = \frac{n+1}{n+2} \left| \frac{1}{2}; \frac{1}{2} \right\rangle \left\langle \frac{1}{2}; \frac{1}{2} \right| + \frac{1}{n+2} \left| \frac{1}{2}; -\frac{1}{2} \right\rangle \left\langle \frac{1}{2}; -\frac{1}{2} \right|.
\end{aligned}
$$

したがって，(4.30) の最小値は $h(\frac{1}{n+2})$ となる．

4.3　群作用の識別

4.3.1　問題の定式化

本節では，表現空間 $\mathcal{H}$ への群 G の（射影的）表現 f が与えられ，未知の要素 $g \in G$ の対象となる物理系 $\mathcal{H}$ への作用 $\mathsf{f}(g)$ が与えられたときに，g を決定する問題を扱う．この場合，系 $\mathcal{H}$ の初期状態 ρ を準備する．すると，未知の作用の後の状態は $\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger$ となる．最後に G に値を持つ POVM M を行い，g を識別する．ここでの議論では（射影的）表現 f は必ずしも既約ではない．後に述べるように，表現空間 $\mathcal{H}$ が複数の既約な表現空間の直和であることが有効に働く．

この問題では，我々の操作は $\mathcal{H}$ 上の初期状態 ρ と $\mathcal{H}$ 上の G に値を持つ POVM M の組 $\mathcal{I} := (\rho, M)$ で与えられる．そして，真の作用が $\mathsf{f}(g)$ であり，推測した作用が $\mathsf{f}(\hat{g})$ であるときの誤差を $R(g, \hat{g})$ とすると，真の作用が $\mathsf{f}(g)$ のとき，操作 $\mathcal{I}$ の性能は，$\mathcal{D}_{R,g}(\mathcal{I}) := \int_G R(g, \hat{g})\, \mathrm{Tr}\, M(dg)\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger$ で与え

られる．そして，4.1.1 項の議論と同様に，mini-max 誤差 $\mathcal{D}_R(\mathcal{I})$ と，事前分布 ν に基づく Bayes 平均誤差 $\mathcal{D}_{R,\nu}(\mathcal{I})$ を以下のように定義する．

$$\mathcal{D}_R(\mathcal{I}) := \max_{g\in G} \mathcal{D}_{R,g}(\mathcal{I}), \quad \mathcal{D}_{R,\nu}(\mathcal{I}) := \int_G \mathcal{D}_{R,g}(\mathcal{I})\nu(dg).$$

事前分布 ν として正規化された不変測度 μ_G の下での Bayes 法または mini-max 法の場合，入力状態 ρ を固定し，M についての最適化を考え，定理 4.1.1 を適用すると，最適な性能 $\min_{\mathcal{I}} \mathcal{D}_R(\mathcal{I}) = \min_{\mathcal{I}} \mathcal{D}_{R,\mu_G}(\mathcal{I})$ を達成する G に値を持つ共変的測定が存在する．また，$\rho = \sum_i p_i|x_i\rangle\langle x_i|$ のとき，$\mathcal{D}_{R,g}(M,\rho) = \sum_i p_i \mathcal{D}_{R,g}(M,|x_i\rangle\langle x_i|)$ となるので，最適な性能 $\min_{\mathcal{I}} \mathcal{D}_R(\mathcal{I}) = \min_{\mathcal{I}} \mathcal{D}_{R,\mu_G}(\mathcal{I})$ を達成する純粋状態 ρ が存在する．したがって，以下では POVM M は共変的測定であり，初期状態は純粋状態 $|x\rangle\langle x|$ である場合に限って議論する．そして，表現空間 $\mathcal{H}$ を $\bigoplus_{\lambda\in S} \mathcal{U}_\lambda \otimes \mathbb{C}^{n_\lambda}$ と表す．ここで，$S \subset \hat{G}$ は $\mathcal{H}$ に現れる既約表現の集合とする．以下では議論の単純化のために，$\mathcal{D}_{R,g}(M_T,\rho)$ を $\mathcal{D}_{R,g}(T,\rho)$ と記す．

以下の議論では共変性から，真の要素 g が単位元である場合だけを扱えば十分である．その場合，群不変性 (4.5) より，

$$R(e, g^{-1}\hat{g}g) = R(g^{-1}, g^{-1}\hat{g}) = R(e,\hat{g}) \tag{4.31}$$

となる．$R(e,\hat{g})$ は実数をとることから，$R(e,\hat{g})$ は既約指標の和 $\sum_\lambda a_\lambda(\chi_\lambda(\hat{g}) + \overline{\chi_\lambda(\hat{g})})$ で表すことができる（[37, 補題 2.8.3] を参照のこと）．

4.3.2 可換群の場合

群 G が可換な場合，既約表現は 1 次元表現となる．したがって，$\lambda \in \hat{G}$ に対応する 1 次元空間の基底を $|\hat{e}_\lambda\rangle$ と書くと純粋状態となる入力状態は $\hat{G}$ 上の二乗可積分空間 $L^2(\hat{G})$ の要素 φ を用いて，$|\varphi\rangle := \sum_{\lambda\in S} \varphi_\lambda |\hat{e}_\lambda\rangle$ と書ける．

そして，共変的 POVM M_T を与える行列 $T \ge 0$ は一般に，$T = \sum_k |\eta_k\rangle\langle\eta_k|$ と書ける．$|\eta_k\rangle = \sum_{\lambda\in S} \sqrt{q_{\lambda,k}} e^{i\theta_{\lambda,k}} |\hat{e}_\lambda\rangle$ とすると，真の群が単位元 e のときの推定値 $\hat{g}$ の分布は $\sum_k |\sum_{\lambda\in S} \mathsf{f}_\lambda(\hat{g}) e^{-i\theta_{\lambda,k}} \sqrt{q_{\lambda,k}} \varphi_\lambda|^2 \mu_G(d\hat{g})$ となる．

この値は，$|\eta_0\rangle = \sum_{\lambda\in S} |\hat{e}_\lambda\rangle$ とし，$T = |\eta_0\rangle\langle\eta_0|$ となる測定を用い，$|\phi_k\rangle := \sum_\lambda e^{-i\theta_{\lambda,k}} \sqrt{q_{\lambda,k}} |\hat{e}_\lambda\rangle$ と置き，入力状態として，混合状態 $\sum_k |\phi_k\rangle\langle\phi_k|$ を用いた場合と一致する．したがって，$T = |\eta_0\rangle\langle\eta_0|$ となる測定に限定しても一

般性を失わない．すなわち，群の作用の識別手法は，入力状態を指定する要素 $\varphi \in L^2(\hat{G})$ を1つ指定することで決まる．このとき，真の群の要素が単位元 e のときの推定値 $\hat{g}$ の分布は φ の逆 Fourier 変換 $\mathcal{F}^{-1}[\varphi]$ を用いて，

$$\left| \sum_{\lambda \in S} \mathsf{f}_\lambda(\hat{g}^{-1})\varphi_\lambda \right|^2 \mu_G(d\hat{g}) = |\mathcal{F}^{-1}[\varphi](\hat{g}^{-1})|^2 \mu_G(d\hat{g})$$

で与えられる．なお，G は非コンパクト群の場合は，$\sum_{\lambda \in S}$ は積分に置き換えられる．

また，利得関数 $\tilde{R}(g, \hat{g})$ が $\hat{G}$ 上の非負の値を持つ関数 a を用いて，$\sum_{\lambda \in \hat{G}} a_\lambda \mathsf{f}_\lambda(g^{-1}\hat{g})$ で与えられるとき，

$$\mathcal{D}_{\tilde{R}}(\varphi) = \sum_{\lambda, \lambda' \in S} a_{\lambda'} \varphi_\lambda \overline{\varphi_{\lambda + \lambda'}} \tag{4.32}$$

となる．

例 4.3.1　$G = \mathbb{R}$ のとき，$L^2(\hat{G}) = L^2(\mathbb{R})$ となり，入力状態は $L^2(\mathbb{R})$ 上の波動関数 $\varphi(\lambda)$ で与えられる．この場合，$\mu_G(d\hat{g}) = \frac{1}{\sqrt{2\pi}} d\hat{g}$, $\mu_{\hat{G}}(d\lambda) = \frac{1}{\sqrt{2\pi}} d\lambda$ となり，$\int_{\mathbb{R}} |\varphi(\lambda)|^2 \frac{1}{\sqrt{2\pi}} d\lambda = 1$ となる．真のパラメータが0であるとき，推定値 $\hat{g} \in \mathbb{R}$ の分布は φ の逆 Fourier 変換 $\mathcal{F}^{-1}[\varphi]$ を用いて，$|\mathcal{F}^{-1}[\varphi](-\hat{g})|^2 \frac{1}{\sqrt{2\pi}} d\hat{g}$ で与えられる．

例えば，定数 E を用いて，条件 $\int \lambda^2 |\varphi(\lambda)|^2 \frac{1}{\sqrt{2\pi}} d\lambda \le E^2$ を課した場合，二乗誤差 $\int \hat{g}^2 |\mathcal{F}^{-1}[\varphi](-\hat{g})|^2 d\hat{g}$ を最小にする φ は $\frac{1}{\sqrt{E}} e^{-\frac{\lambda^2}{4E^2}}$ で与えられる．このとき，その逆 Fourier 変換は $\sqrt{2E} e^{-E^2\lambda^2}$ となり，二乗誤差の最小値 $\frac{1}{4E^2}$ を与える．

また，$\varphi(\lambda)$ として，そのサポートが閉区間上 $[-1, 1]$ に含まれるものに限った場合，二乗誤差を最小にする φ は閉区間上 $[-1, 1]$ で $(2\pi)^{1/4} \sin \frac{\pi(1+\lambda)}{2}$ で与えられる．このとき，その逆 Fourier 変換は $-\frac{\pi^{3/4}}{2^{1/4}} \frac{\cos \hat{g}}{\hat{g}^2 - \pi^2/4}$ となり，二乗誤差の最小値 $\frac{\pi^2}{4}$ を与える．

ここで，以下の例を扱うために以下の定理を準備する．

定理 4.3.2　([19])　$n \times n$ 行列 $P_n := \sum_{k=1}^{n-1} |k\rangle\langle k+1| + |k+1\rangle\langle k|$ の固

有値は $2\cos\frac{j\pi}{n+1}$ $(j=1,\ldots,n)$ であり，対応する固有ベクトル $\vec{x}$ は $x^j := \sum_{k=1}^n \sin\frac{jk\pi}{n+1}|k\rangle$ で与えられる．

例 4.3.3　$G=U(1)=\{e^{i\theta}\,|\,\theta\in[0,2\pi]\}$ のとき，表現は 整数 λ を用いて，$e^{\lambda i\theta}$ で与えられる．よって，$L^2(\hat{G})=L^2(\mathbb{Z})$ となり，入力状態は $L^2(\mathbb{Z})$ 上の波動関数 $\varphi(\lambda)$ で与えられる．真のパラメータが 0 であるとき，推定値 $\hat{\theta}\in\mathbb{R}$ の分布は φ の逆 Fourier 変換 $\mathcal{F}^{-1}[\varphi]$ を用いて，$|\mathcal{F}^{-1}[\varphi](-\hat{\theta})|^2 d\hat{\theta}$ で与えられる．もし，$\varphi(\lambda)$ のサポートをいくらでも広くとると，誤差はいくらでも小さくなる．したがって，入力状態のサポートが $\{k\in\mathbb{Z}|\ |k|\le n\}$ に制限された場合について扱う．

利得関数 $\tilde{R}(\theta,\hat{\theta})$ が $\cos(\theta-\hat{\theta})=(e^{i(\theta-\hat{\theta})}+e^{i(\theta-\hat{\theta})})/2=1-2\sin^2(\frac{\theta-\hat{\theta}}{2})$ で与えられるときを考える．すなわち，誤差関数が $2\sin^2(\frac{\theta-\hat{\theta}}{2})$ で与えられたとする．入力状態を $(\varphi(\lambda))_{\lambda=-n}^n$ とすると，(4.32) より，利得は

$$\sum_{\lambda=-n}^{n-1}\frac{1}{2}\varphi(\lambda)\varphi(\lambda+1)+\sum_{\lambda=-n+1}^{n}\frac{1}{2}\varphi(\lambda-1)\varphi(\lambda)=\sum_{\lambda=-n}^{n-1}\varphi(\lambda)\varphi(\lambda+1)$$

となる．ここで定理 4.3.2 より，この値を最大にする $(\varphi(\lambda))$ は $\varphi(\lambda)=\sin\frac{\pi(\lambda+n+1)}{2n+2}$ であり，最大値は $\cos\frac{\pi}{2n+2}$ となる．

一方，$n\to\infty$ の極限では，入力状態 $\varphi_n(\lambda)$ は閉区間上 $[-1,1]$ の二乗可積分関数 $\hat{\varphi}\in L^2([-1,1])$ を用いて，近似的に $\varphi_n(\lambda)=\frac{1}{\sqrt{n}}\hat{\varphi}(\lambda/n)$ で与えることができる．この入力の下，真のパラメータが 0 であるとき，確率変数である推定値 $\hat{\theta}$ は 0 に確率収束する．したがって，確率変数 $x:=n\hat{\theta}$ に注目すると，$dx=nd\hat{\theta}$ であるので，このとき，$y=-\lambda/n$ とすると，

$$\lim_{n\to\infty}\frac{1}{n}|\mathcal{F}^{-1}[\varphi_n](-nx)|^2dx=\lim_{n\to\infty}\frac{1}{n}\left|\sum_{\lambda=-n}^{n}\frac{1}{\sqrt{n}}\hat{\varphi}(\lambda/n)e^{-i\frac{x}{n}\lambda}\right|^2dx$$

$$=\left|\lim_{n\to\infty}\frac{1}{n}\sum_{\lambda=-n}^{n}\hat{\varphi}(\lambda/n)e^{-i\frac{x}{n}\lambda}\right|^2dx=\left|\int_{-1}^{1}\hat{\varphi}(y)e^{-ixy}dy\right|^2dx$$

$$=2\pi|\mathcal{F}^{-1}[\hat{\varphi}](-x)|^2dx$$

となり，$\hat{\varphi}$ の逆 Fourier 変換 $\mathcal{F}^{-1}[\hat{\varphi}]$ を用いて表すことができる．すなわち，

$G=\mathbb{R}$ のときの $\varphi(\lambda)$ のサポートが閉区間上 $[-1,1]$ に制限された問題に帰着される．

そして，誤差関数は $2\sin^2(\frac{\theta-\hat{\theta}}{2})n^2 \cong \frac{(\theta-\hat{\theta})^2 n^2}{2} = x^2/2$ と近似できるので，関数 $f \in L^2(\mathbb{R})$ のサポートが閉区間上 $[-1,1]$ に制限され，誤差関数が x^2 となる場合に帰着される．

4.3.3　非可換群での逆 Fourier 変換の役割

共変的 POVM M_T を与える行列 $T \ge 0$ は一般に，$T=\sum_k |\eta_k\rangle\langle\eta_k|$ と書ける．真の群の作用が単位元の作用で与えられているとき，推定値 $\hat{g}$ の分布は以下のように変形できる．ただし，以下では $|x\rangle = \sum_\lambda |X_\lambda\rangle\rangle$, $|\eta_k\rangle = \sum_\lambda |\eta_{k,\lambda}\rangle\rangle$, $|x_k\rangle := \sum_\lambda \frac{1}{\sqrt{d_\lambda}}|X_\lambda \eta_{k,\lambda}^\dagger\rangle\rangle$, $|I\rangle := \sum_\lambda \sqrt{d_\lambda}|I_\lambda\rangle\rangle$ と置く．

$$\sum_k |\langle\eta_k|\mathsf{f}(\hat{g}^{-1})|x\rangle|^2 \mu_G(d\hat{g}) = \sum_k \left| \sum_{\lambda\in S} \mathrm{Tr}\, \eta_{k,\lambda}^\dagger \mathsf{f}_\lambda(\hat{g}^{-1}) X_\lambda \right|^2 \mu_G(d\hat{g})$$

$$= \sum_k \left| \sum_{\lambda\in S} \mathrm{Tr}\, \mathsf{f}_\lambda(\hat{g}^{-1}) X_\lambda \eta_{k,\lambda}^\dagger \right|^2 \mu_G(d\hat{g}) = \sum_k |\langle I|\mathsf{f}(\hat{g}^{-1})|x_k\rangle\rangle|^2 \mu_G(d\hat{g}).$$

(4.15) より，

$$\sum_k \mathrm{Tr}\,|x_k\rangle\langle x_k| = \sum_k \sum_\lambda \frac{1}{d_\lambda} \mathrm{Tr}\, \eta_{k,\lambda} X_\lambda^\dagger X_\lambda \eta_{k,\lambda}^\dagger = \sum_\lambda \mathrm{Tr}\, X_\lambda^\dagger X_\lambda \sum_k \frac{1}{d_\lambda} \eta_{k,\lambda}^\dagger \eta_{k,\lambda}$$

$$= \sum_\lambda \mathrm{Tr}\, X_\lambda^\dagger X_\lambda I_{n_\lambda} = \mathrm{Tr}\,|x\rangle\langle x| = 1$$

となる．したがって，混合状態 $\sum_k |x_k\rangle\langle x_k|$ を入力状態とし，行列 $|I\rangle\langle I|$ から得られる共変的測定を行った場合に帰着できる．

したがって，適当に k を選ぶと

$$\mathcal{D}_{R,\mu_G}\left(|I\rangle\langle I|, \frac{1}{\langle x_k|x_k\rangle}|x_k\rangle\langle x_k|\right) \le \mathcal{D}_{R,\mu_G}(|I\rangle\langle I|, \sum_k |x_k\rangle\langle x_k|)$$

$$= \mathcal{D}_{R,\mu_G}(T, |x\rangle\langle x|)$$

が成り立つ．そして，行列 $X_\lambda \eta_{k,\lambda}^\dagger$ のランクは高々 n_λ であるので，純粋状態 $\frac{1}{\langle x_k|x_k\rangle}|x_k\rangle\langle x_k|$ は $\mathcal{H}$ 上の状態と見なすことができる．よって，以下

の議論では，測定は，$|I\rangle\langle I|$ で生成される共変的測定で与えられ，入力状態は $\mathcal{H}$ 上の純粋状態 $|x\rangle$ の場合に限ることにする．ここで，$\mathcal{U}_\lambda$ 上の行列（無限次元の場合は Hilbert Schmidt 作用素）からなる空間を $\mathfrak{gl}(\mathcal{U}_\lambda)$ とし，$L^2(\hat{G}) := \bigoplus_\lambda \mathfrak{gl}(\mathcal{U}_\lambda)$ を考える．（より詳しくは [37, 3.8 節] を参照のこと．）そして，$L^2(\hat{G})$ の要素 $X = (X_\lambda)_{\lambda^\dagger}$ で行列 X_λ のランクが表現空間 $\mathcal{H}$ での既約表現 $\mathcal{U}_\lambda$ の重複度 n_λ 以下となるものの集合を $L^2(\hat{G}) \wedge \mathcal{H}$ 記す．すると，$|x\rangle = \sum_\lambda |X_\lambda\rangle\rangle$ となるように行列のなすベクトル $X = (X_\lambda)_{\lambda^\dagger}$ を選ぶと，X は $L^2(\hat{G}) \wedge \mathcal{H}$ の要素と見なすことができる．したがって，真の群の作用が単位元の作用で与えられているとき，推定値 $\hat{g}$ の分布は X の逆 Fourier 変換 $\mathcal{F}^{-1}[X] := \sum_{\lambda\in\hat{G}} \sqrt{d_\lambda}\,\mathrm{Tr}\,\mathsf{f}_\lambda(\hat{g}^{-1})X_\lambda$ を用いて，以下のように与えられる．

$$
\begin{aligned}
|\langle I|\mathsf{f}_\lambda(\hat{g}^{-1})|x\rangle|^2\mu_G(d\hat{g}) &= \Big|\sum_{\lambda\in S}\sqrt{d_\lambda}\,\mathrm{Tr}\,\mathsf{f}_\lambda(\hat{g}^{-1})X_\lambda\Big|^2\mu_G(d\hat{g}) \\
&= |\mathcal{F}^{-1}[X](\hat{g}^{-1})|^2\mu_G(d\hat{g}).
\end{aligned}
$$

したがって，以下の定理を得る．

定理 4.3.4 $X \in L^2(\hat{G})$ について $\mathcal{D}_R(X) := \int_G R(e,\hat{g})|\mathcal{F}^{-1}[X](\hat{g}^{-1})|^2 \mu_G(d\hat{g})$ とすると，$\min_{M,\rho}\mathcal{D}_R(M,\rho) = \min_{X\in L^2(\hat{G})\wedge\mathcal{H}, \|X\|_{L^2(\hat{G})}=1}\mathcal{D}_R(X)$ となる．

4.3.4 有限群の場合

以下では G が有限群であり，エラー関数 R が

$$
R(g,\hat{g}) := \begin{cases} 1 & \text{if } \hat{g} \neq g \\ 0 & \text{if } \hat{g} = g \end{cases}
$$

で与えられている場合について，$\mathcal{H} = \bigoplus_{\lambda\in S}\mathcal{U}_\lambda \otimes \mathbb{C}^{n_\lambda}$ 上の最適な入力状態に対応する $X \in L^2(\hat{G}) \wedge \mathcal{H}$ を求める．正しく識別する確率は

$$
\mathcal{D}_{1-R}(X) = \frac{|\mathcal{F}^{-1}[X](e)|^2}{|G|} = \frac{|\sum_{\lambda\in S}\sqrt{d_\lambda}\,\mathrm{Tr}\,X_\lambda|^2}{|G|}
$$

となる．したがって，空間 $L^2(\hat{G})$ についての Schwarz の不等式より，

$$
\frac{|\sum_{\lambda\in S}\sqrt{d_\lambda}\,\mathrm{Tr}\,X_\lambda|^2}{|G|} = \frac{|\sum_{\lambda\in S}\mathrm{Tr}\,\sqrt{d_\lambda}I_{\min\{d_\lambda,n_\lambda\}}X_\lambda|^2}{|G|}
$$

$$\leq \frac{(\sum_{\lambda\in S}\mathrm{Tr}\, d_\lambda I_{\min\{d_\lambda,n_\lambda\}})(\sum_{\lambda\in S}\mathrm{Tr}\, X_\lambda^\dagger X_\lambda)}{|G|} = \frac{\sum_{\lambda\in S} d_\lambda \min\{d_\lambda, n_\lambda\}}{|G|}$$

となる．また，等号を達成する X は $(\frac{1}{\sum_{\lambda\in S} d_\lambda \min\{d_\lambda,n_\lambda\}}\sqrt{d_\lambda} I_{\min\{d_\lambda,n_\lambda\}})$ で与えられる．すなわち，最適識別確率は $\mathcal{D}(S,\{n_\lambda\}_{n\in S}) := \frac{\sum_{\lambda\in S} d_\lambda \min\{d_\lambda,n_\lambda\}}{|G|}$ で与えられる [35]．特に，全ての既約表現 $\lambda\in\hat{G}$ が重複度 d_λ で準備された場合には，確率 1 で作用を同定することができる．

例 4.3.5　(稠密度符号化 [6, 32])　群 $\mathbb{F}_q^{2r}$ に対する離散 Heisenberg 表現 $\mathsf{W}_{\mathbb{F}}^r$ を考える．このとき，重複度が 1 であるとすると，最適識別確率は

$$\frac{q^r}{q^{2r}} = \frac{1}{q^r} \tag{4.33}$$

となる．群 $\mathbb{Z}_d^{2r}$ の場合，この値は $\frac{d^r}{d^{2r}} = \frac{1}{d^r}$ となる．

一方，自由に参照系が使え，重複度が表現空間と同じ場合，$\mathbb{F}_q^{2r}$ のときの最適識別確率は

$$\frac{q^{2r}}{q^{2r}} = 1 \tag{4.34}$$

となる．群 $\mathbb{Z}_d^{2r}$ の場合，この値は $\frac{d^{2r}}{d^{2r}} = 1$ となる．この事実は，参照系を利用することで識別確率が格段に向上することを示している．

この事実は以下のよう通信に応用できる．最初に最大エンタングル状態を準備し，参照系を受信者にあらかじめ送っておく．送信者は表現空間に群 $\mathbb{F}_q^{2r}$ または群 $\mathbb{Z}_d^{2r}$ の作用を施した後に，その表現空間に対応する物理系を受信者に送る．受信者が，合成系を表現に対応する基底で測ることで，q^r (d^r) 次元の伝送だけで，q^{2r} (d^{2r}) の情報が伝送できる．

以下，記述の単純化のために，群 $\mathbb{F}_q^{2r}$ と群 $\mathbb{Z}_d^{2r}$ について共通の事項を扱う場合，これらの群を一般的に $\mathbb{X}$ と記すことにする．例えば，射影的ユニタリ表現 $\mathsf{W}_{\mathbb{X}}^r$ は $\mathbb{X}=\mathbb{F}$ のときは，射影的ユニタリ表現 $\mathsf{W}_{\mathbb{F}}^r$ を意味し，$\mathbb{X}=\mathbb{Z}$ のときは，射影的ユニタリ表現 $\mathsf{W}_{\mathbb{Z}}^r$ を意味することとする．そして，$\mathsf{W}_{\mathbb{X}}^r$ と交換関係が因子団を除き同一で因子団が $\mathsf{W}_{\mathbb{X}}^r$ の因子団の二乗でとなる射影的ユニタリ表現を $\mathsf{W}_{\mathbb{X}:2}^r$ と記す．すると，q または d が奇数の場合は，射影的ユニタリ表現 $(\mathsf{W}_{\mathbb{X}}^r)^{\otimes 2}$ の既約分解は $\mathsf{W}_{\mathbb{X}:2}^r$ が重複度 $|\mathbb{X}|^r$ で現れる．

したがって，射影的ユニタリ表現 $\mathsf{W}^r_{\mathbb{X}:2}$ に上記の議論を適用すると，確率 1 で群の作用が決定できる．

例 4.3.6 （離散シンプレクティク群）　離散シンプレクティク群 $\mathrm{Sp}(2r,\mathbb{F}_q)$ のメタプレクティク表現 $\mathsf{S}^r_{\mathbb{F}_q}$ に注目する．重複度が 1 であるとすると，最適識別確率は

$$\frac{q^r}{q^{r^2}\prod_{k=1}^r(q^{2k}-1)} = \frac{1}{q^{r^2-r}\prod_{k=1}^r(q^{2k}-1)} \tag{4.35}$$

となる．特に，$r=1$ の場合は $\frac{1}{q^2-1}$ となる．

一方，自由に参照系が使え，重複度が表現空間と同じまでとれる場合，最適識別確率は $p \neq 2$ のとき，

$$\frac{(\frac{q^r+1}{2})^2+(\frac{q^r-1}{2})^2}{q^{r^2}\prod_{k=1}^r(q^{2k}-1)} = \frac{q^{2r}+1}{2q^{r^2}\prod_{k=1}^r(q^{2k}-1)} \tag{4.36}$$

となり，特に，$r=1$ の場合は $\frac{q^2+1}{2(q^2-1)}$ となる．$p=2$ のとき，

$$\frac{q^{2r}}{q^{r^2}\prod_{k=1}^r(q^{2k}-1)} = \frac{1}{q^{r^2-2r}\prod_{k=1}^r(q^{2k}-1)} \tag{4.37}$$

となり，特に，$r=1$ の場合は $\frac{q}{q^2-1}$ となる．特に，$q=2$ のときは，$\mathrm{Sp}(2r,\mathbb{F}_q)$ は S_3 となり，$\frac{2}{3}$ となる．

例 4.3.7 （$\mathbb{F}_q^{2r}$ 上の Clifford 群）　Clifford 群 $\mathbb{F}_q^{2r} \rtimes \mathrm{Sp}(2r,\mathbb{F}_q)$ の表現 $\mathsf{V}^r_{\mathbb{F}} \otimes \overline{\mathsf{V}^r_{\mathbb{F}}}$ に注目する．ここで，$\bar{\mathsf{f}}$ は f の複素共役表現を表す．重複度が 1 であるとすると，最適識別確率は

$$\frac{q^{2r}}{q^{r^2+2}\prod_{k=1}^r(q^{2k}-1)} = \frac{1}{q^{r^2}\prod_{k=1}^r(q^{2k}-1)} \tag{4.38}$$

となる．特に，$r=1$ の場合は $\frac{1}{q(q^2-1)}$ となる．一方，自由に参照系が使え，重複度が表現空間と同じまでとれる場合，最適識別確率は

$$\frac{1+(q^{2r}-1)^2}{q^{r^2+2}\prod_{k=1}^r(q^{2k}-1)} \tag{4.39}$$

となり，特に，$r=1$ の場合は $\frac{q^4-2q^2+2}{q^3(q^2-1)}$ となる．

表現 $\mathsf{V}_{\mathbb{F}}^r \otimes \mathsf{V}_{\mathbb{F}}^r$ の場合，重複度が 1 の場合は，最適識別確率は (4.38) に等しい．しかし，自由に参照系が使え，重複度が表現空間と同じ大きさまでとれる場合，最適識別確率は

$$\frac{(\frac{q^r(q^r+1)}{2})^2 + (\frac{q^r(q^r-1)}{2})^2}{q^{r^2+2}\prod_{k=1}^r (q^{2k}-1)} = \frac{q^{2r}+1}{2q^{r^2}\prod_{k=1}^r (q^{2k}-1)} \tag{4.40}$$

となり，特に，$r=1$ の場合は $\frac{q^2+1}{2q(q^2-1)}$ となる．

例 4.3.8 （直積群 $\mathbb{F}_q^{2r} \times \mathrm{Sp}(\mathbb{F}_q, 2r)$）　表現 $\mathsf{V}_{\mathbb{F}}^r \otimes \overline{\mathsf{V}_{\mathbb{F}}^r}$, $\mathsf{V}_{\mathbb{F}}^r \otimes \mathsf{V}_{\mathbb{F}}^r$ との比較のため，直積群 $\mathbb{F}_q^{2r} \times \mathrm{Sp}(\mathbb{F}_q, 2r)$ の表現 $\mathsf{W}_{\mathbb{F}}^r \overline{\otimes} \mathsf{S}_{\mathbb{F}}^r$ （もしくは $\mathsf{W}_{\mathbb{F}}^r \overline{\otimes} \overline{\mathsf{S}_{\mathbb{F}}^r}$, $\overline{\mathsf{W}_{\mathbb{F}}^r} \overline{\otimes} \mathsf{S}_{\mathbb{F}}^r$, $\overline{\mathsf{W}_{\mathbb{F}}^r} \overline{\otimes} \overline{\mathsf{S}_{\mathbb{F}}^r}$）による作用を識別する場合を考える．この場合，上記 4 つの表現での既約部分空間の次元は同じである．したがって，$\mathsf{W}_{\mathbb{F}}^r \overline{\otimes} \mathsf{S}_{\mathbb{F}}^r$ のみ扱う．この問題は，個別に 2 つの群 $\mathbb{F}_q^{2r}$, $\mathrm{Sp}(\mathbb{F}_q, 2r)$ の作用が与えられたときに，個別に識別することと同じである．したがって，個別の正しく識別する確率の積に一致する．

重複度が 1 の場合，両者の作用を正しく識別する確率は (4.38) と一致する．したがって，$\mathsf{V}_{\mathbb{F}}^r \otimes \overline{\mathsf{V}_{\mathbb{F}}^r}$, $\mathsf{V}_{\mathbb{F}}^r \otimes \mathsf{V}_{\mathbb{F}}^r$, $\mathsf{W}_{\mathbb{F}}^r \overline{\otimes} \mathsf{S}_{\mathbb{F}}^r$ の間には差が生じない．

一方，自由に参照系が使え，重複度が表現空間と同じまでとれる場合，(4.34) が 1 であるから，最適識別確率は $p \neq 2$ の場合，(4.36) となり，$p=2$ の場合，(4.37) となる．$p \neq 2$ の場合，(4.40) と (4.36) は一致する．このため，$\mathsf{W}_{\mathbb{F}}^r \overline{\otimes} \mathsf{S}_{\mathbb{F}}^r$ の場合と，$\mathsf{V}_{\mathbb{F}}^r \otimes \mathsf{V}_{\mathbb{F}}^r$ の場合は一致する．しかし，

$$\frac{1+(q^{2r}-1)^2}{q^{r^2+2}\prod_{k=1}^r (q^{2k}-1)} > \frac{q^{2r}+1}{2q^{r^2}\prod_{k=1}^r (q^{2k}-1)} \tag{4.41}$$

であるので，表現 $\mathsf{V}_{\mathbb{F}}^r \otimes \overline{\mathsf{V}_{\mathbb{F}}^r}$ の場合の方が真に正しく識別する確率は向上する．

$p=2$ の場合，(4.37), (4.39), (4.40) の間には以下の関係がある．

$$\frac{1}{q^{r^2-2r}\prod_{k=1}^r (q^{2k}-1)} > \frac{1+(q^{2r}-1)^2}{q^{r^2+2}\prod_{k=1}^r (q^{2k}-1)} > \frac{q^{2r}+1}{2q^{r^2}\prod_{k=1}^r (q^{2k}-1)}. \tag{4.42}$$

したがって，$\mathsf{W}_{\mathbb{F}}^r \overline{\otimes} \mathsf{S}_{\mathbb{F}}^r$ の場合が最もよく，その次に，表現 $\mathsf{V}_{\mathbb{F}}^r \otimes \overline{\mathsf{V}_{\mathbb{F}}^r}$ がよく，$\mathsf{V}_{\mathbb{F}}^r \otimes \mathsf{V}_{\mathbb{F}}^r$ が最も悪いことがわかる．

例 4.3.9 （$\mathbb{Z}_d^2$ 上の Clifford 群） Clifford 群 $\mathbb{Z}_d^2 \rtimes \mathrm{Sp}(2,\mathbb{Z}_d)$ の表現 $\mathsf{V}_{\mathbb{Z}}^r \otimes \overline{\mathsf{V}_{\mathbb{Z}}^r}$ に注目する．今，簡単のため，d は素数 p の冪 p^k であるとする．重複度が 1 であるとすると，最適識別確率は $\frac{p^{2k}}{p^{5k}(1-p^{-2})}$ となる．一方，自由に参照系が使え，重複度が表現空間の次元までとれる場合，最適識別確率は

$$\frac{p^{4(k-1)}(p^2-1)^2 + p^{4(k-2)}(p^2-1)^2 + \cdots + (p^2-1)^2 + 1}{p^{5k}(1-p^{-2})}$$
$$= \frac{\frac{(p^2-1)(p^{4k}-1)}{p^2+1} + 1}{p^{5k}(1-p^{-2})} = \frac{p^{4k}(p^2-1)+2}{p^{5k-2}(p^4-1)}$$

となる．

例 4.3.10 （置換群 [79, 35, 32]） 置換群 S_n が $(\mathbb{C}^d)^{\otimes n}$ に対して，テンソル積の順番についての置換として作用する場合を考えよう．このとき，$(\mathbb{C}^d)^{\otimes n}$ の他に，十分な次元の参照系が準備されており，それとのエンタングルメントは自由に用いることができるとする．このとき，最適な初期状態を準備し，最適な測定を用いたとすると，正しく置換群 S_n の作用を識別する確率は Plancherel 測度 $\mu_n(d)$ によって与えられる．したがって，n が十分大きい極限においては，次元 d は $2\sqrt{n}$ ぐらいあれば十分であることがわかる．([37] の 2.9 節を参照) より詳細な次元 d に応じた漸近的な成功確率については [37] の式 (2.60) によって扱うことができる．

4.3.5 一般のコンパクト Lie 群の場合

以下，一般のコンパクト Lie 群の場合に，最適な入力状態に対応する $X \in L^2(\hat{G}) \wedge \mathcal{H}$ を求める．そのため，表現空間の既約分解 $\mathcal{H} = \bigoplus_{\boldsymbol{\lambda} \in S} \mathcal{U}_{\boldsymbol{\lambda}} \otimes \mathbb{C}^{n_{\boldsymbol{\lambda}}}$ に注目し，(ただし，$S := \{\boldsymbol{\lambda} \in \hat{G} \,|\, n_{\boldsymbol{\lambda}} \neq 0\}$) 解析を簡単にするため，任意の $\boldsymbol{\lambda} \in S$ に対して $n_{\boldsymbol{\lambda}} \geq d_{\boldsymbol{\lambda}}$ を仮定する．

そして，$g \in G$ に対して，$X_g := (\mathsf{f}_{\boldsymbol{\lambda}}(g) X_{\boldsymbol{\lambda}} \mathsf{f}_{\boldsymbol{\lambda}}(g^{-1}))_{\boldsymbol{\lambda}} \in L^2(\hat{G})$ を定義すると，(4.31) より，

$$\mathcal{D}_R(X) = \int_G R(e,\hat{g}) |\mathcal{F}^{-1}[X](\hat{g}^{-1})|^2 \mu_G(d\hat{g})$$
$$= \int_G R(e, g^{-1}\hat{g}g) |\mathcal{F}^{-1}[X](\hat{g}^{-1})|^2 \mu_G(d\hat{g})$$

$$= \int_G R(e, \hat{g}) |\mathcal{F}^{-1}[X](g\hat{g}^{-1}g^{-1})|^2 \mu_G(d\hat{g})$$

$$= \int_G R(e, \hat{g}) |\mathcal{F}^{-1}[X_{g^{-1}}](\hat{g}^{-1})|^2 \mu_G(d\hat{g}) = \mathcal{D}_R(X_{g^{-1}}) \tag{4.43}$$

が成り立つ．

以下，エラー関数 R が自明でない既約表現の指標を用いて

$$R(g, \hat{g}) = -\sum_{\boldsymbol{\lambda} \in \hat{G}} a_{\boldsymbol{\lambda}} (\chi_{\boldsymbol{\lambda}}(\hat{g}g^{-1}) + \chi_{\boldsymbol{\lambda}^*}(\hat{g}g^{-1})), \quad a_{\boldsymbol{\lambda}} = a_{\boldsymbol{\lambda}^*} \geq 0 \tag{4.44}$$

と書ける場合を考える．この問題は利得関数

$$\tilde{R}(g, \hat{g}) = \sum_{\boldsymbol{\lambda} \in \hat{G}} a_{\boldsymbol{\lambda}} (\chi_{\boldsymbol{\lambda}}(\hat{g}g^{-1}) + \chi_{\boldsymbol{\lambda}^*}(\hat{g}g^{-1})), \quad a_{\boldsymbol{\lambda}} = a_{\boldsymbol{\lambda}^*} \geq 0 \tag{4.45}$$

を最大化する問題と同じである．

例えば，正しく識別する確率を利得関数とした場合は，$R(g, \hat{g})$ として，$\delta_{g,\hat{g}}$ を選んだ場合となる．$G = \mathrm{SU}(d)$ の場合，利得関数として，Gate fidelity $|\operatorname{Tr} g^\dagger \hat{g}|^2$ が用いられる．$d = 2$ のとき，この値は $1 + \chi_1(g) = 1 + \chi_{(2,0)}(g) = 1 + \chi_{[2]}(g)$ となる．一方，$d > 2$ のとき，この値は $1 + \chi_{[1,0,\ldots,0,1]}(g)$ と等しくなり，(4.45) を満たす．

そして，$\mathcal{U}_{\boldsymbol{\lambda}} \otimes \mathbb{C}^{d_{\boldsymbol{\lambda}}}$ 上のエンタングル状態 $|\Psi_{\boldsymbol{\lambda}}\rangle\rangle := \frac{1}{\sqrt{d_{\boldsymbol{\lambda}}}} \sum_{j=1}^{d_{\boldsymbol{\lambda}}} |\boldsymbol{\lambda}; j; j\rangle$ を用いると以下の定理が成り立つ．ただし，$|\boldsymbol{\lambda}; j; j\rangle = |\boldsymbol{\lambda}; j\rangle \otimes |j\rangle$ である．

定理 4.3.11 （[16]）　$X \in L^2(\hat{G})$ に対して，表現 $\boldsymbol{\lambda} \in \hat{G}$ 上の行列 $\Phi_{\boldsymbol{\lambda}}$ と非負の実数 $c_{\boldsymbol{\lambda}} \geq 0$ で $X = (c_{\boldsymbol{\lambda}} \Phi_{\boldsymbol{\lambda}})_{\boldsymbol{\lambda}}$ および $\operatorname{Tr} \Phi_{\boldsymbol{\lambda}}^\dagger \Phi_{\boldsymbol{\lambda}} = 1$ を満たすものを選ぶ．このとき，誤差関数を (4.44) で与えると，

$$\mathcal{D}_R(X) \geq -\sum_{\boldsymbol{\lambda}, \boldsymbol{\lambda}' \in S} c_{\boldsymbol{\lambda}} c_{\boldsymbol{\lambda}'} \sum_{\boldsymbol{\lambda}'' \in \hat{G}} a_{\boldsymbol{\lambda}''} (C^{\boldsymbol{\lambda}''*}_{\boldsymbol{\lambda}, \boldsymbol{\lambda}'*} + C^{\boldsymbol{\lambda}''}_{\boldsymbol{\lambda}, \boldsymbol{\lambda}'*})$$

$$= -\sum_{\boldsymbol{\lambda}'' \in \hat{G}} a_{\boldsymbol{\lambda}''} \sum_{\boldsymbol{\lambda}, \boldsymbol{\lambda}' \in S} (C^{\boldsymbol{\lambda}'}_{\boldsymbol{\lambda}'', \boldsymbol{\lambda}} + C^{\boldsymbol{\lambda}'}_{\boldsymbol{\lambda}''*, \boldsymbol{\lambda}}) c_{\boldsymbol{\lambda}} c_{\boldsymbol{\lambda}'} \tag{4.46}$$

が成り立つ．等号は $X = (c_{\boldsymbol{\lambda}} \Psi_{\boldsymbol{\lambda}})_{\boldsymbol{\lambda}}$ のとき成り立つ．このときの (4.46) の値を $\mathcal{D}_R(\{c_{\boldsymbol{\lambda}}\})$ と表し，$\mathcal{F}^{-1}[X] = \sum_{\boldsymbol{\lambda}} c_{\boldsymbol{\lambda}} \chi_{\boldsymbol{\lambda}}$ が成り立つ．

したがって，表現空間 $\bigoplus_{\boldsymbol{\lambda}\in S}\mathcal{U}_{\boldsymbol{\lambda}}\otimes\mathbb{C}^{d_{\boldsymbol{\lambda}}}$ である場合の最適な識別手法を選ぶ問題は (4.46) を最大にする $c=(c_{\boldsymbol{\lambda}})_{\boldsymbol{\lambda}\in S}$ を選ぶ問題に帰着される．

ここで定理 4.3.11 の意味で最適性能を実現する POVM は必ずしも G について共変的である必要はない．G 上の測度 ν について以下の定理を紹介する [37, 定理 4.5.1].

定理 4.3.12　G 上の測度 ν と G の表現 $\mathsf{f}_{\boldsymbol{\lambda}}$ について，以下の条件は同値である．ただし，表現空間 $\mathcal{H}$ が無限次元となるときは，その全ての既約成分は形式的次元を持つとする．

(1)　$\int_G \mathsf{f}_{\boldsymbol{\lambda}}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger\mu_G(dg)=\int_G \mathsf{f}_{\boldsymbol{\lambda}}(g)\otimes\mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger\nu(dg)$.

(2)　任意の行列 X について $\int_G \mathsf{f}_{\boldsymbol{\lambda}}(g)X\mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger\mu_G(dg)=\int_G \mathsf{f}_{\boldsymbol{\lambda}}(g)X\mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger\nu(dg)$ が成り立つ．（表現空間が無限次元の場合は，任意のトレースクラス作用素 X について上の式が成り立つ．）

(3)　任意のエルミート行列 X について $\int_G \mathsf{f}_{\boldsymbol{\lambda}}(g)X\mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger\mu_G(dg)=\int_G \mathsf{f}_{\boldsymbol{\lambda}}(g)$ $X\mathsf{f}_{\boldsymbol{\lambda}}(g)^\dagger\nu(dg)$ が成り立つ．（表現空間が無限次元の場合は，任意のトレースクラス自己共役作用素 X について上の式が成り立つ．）

そして，G 上の測度 ν が任意の $\lambda\in S$ について上記の定理の条件を満たすとき，S-design とよぶ．S-design となる G 上の測度 ν について，積分 $\int_G \mathsf{f}(\hat{g})|I\rangle\langle I|\mathsf{f}(\hat{g})^{-1}\nu(d\hat{g})=I$ は POVM を与えるので，その POVM を $M(\nu)$ と記す．したがって，入力状態として，$X=(c_{\boldsymbol{\lambda}}\Psi_{\boldsymbol{\lambda}})_{\boldsymbol{\lambda}}$ から定義される状態を用い，上記の測定を用いる推定方法が存在する．ここで，$S'':=\{\boldsymbol{\lambda}''\in\hat{G}\,|\,\boldsymbol{\lambda}''\neq 0, a_{\boldsymbol{\lambda}''}>0\}$, $S':=\{\boldsymbol{\lambda}'\in S\,|\,\exists\boldsymbol{\lambda}\in S,\exists\boldsymbol{\lambda}''\in S, C^{\boldsymbol{\lambda}'}_{\boldsymbol{\lambda},\boldsymbol{\lambda}''}\neq 0\}$ とする．ν が $S\cup S'$-design であるとする．このとき，[37] の補題 4.5.2 より，ν_g も $S\cup S'$-design となり，[37] の補題 4.5.3 より，

$$
\begin{aligned}
&\mathcal{D}_{R,g}(M(\nu),|X\rangle)\\
&=\int_{G'}-\sum_{\boldsymbol{\lambda}''\in\hat{G}}a_{\boldsymbol{\lambda}''}(\chi_{\boldsymbol{\lambda}''}(\hat{g}'g^{-1})+\chi_{\boldsymbol{\lambda}''*}(\hat{g}'g^{-1}))\left|\sum_{\boldsymbol{\lambda}\in S}c_{\boldsymbol{\lambda}}\chi_{\boldsymbol{\lambda}}(\hat{g}'g^{-1})\right|^2\mu_{G'}(d\hat{g}')\\
&=-\sum_{\boldsymbol{\lambda},\boldsymbol{\lambda}'\in S}c_{\boldsymbol{\lambda}}c_{\boldsymbol{\lambda}'}\sum_{\boldsymbol{\lambda}''\in\hat{G}}a_{\boldsymbol{\lambda}''}(C^{\boldsymbol{\lambda}''*}_{\boldsymbol{\lambda},\boldsymbol{\lambda}'*}+C^{\boldsymbol{\lambda}''}_{\boldsymbol{\lambda},\boldsymbol{\lambda}'*})
\end{aligned}
$$

が成り立つ．したがって，群 G が連続な一般の Lie 群であっても，$S\cup S'$-

design となる有限部分群 G' を見つけることで，離散個の値を持つ POVM で最適なものが実現できる．

なお，射影的表現の場合は $\mathcal{E}$ をある因子団とすると，S は $\hat{G}[\mathcal{E}]$ の部分集合となる．このように置き換えることで，以下の証明は成り立つので，定理 4.3.11 はそのまま成り立つ．

証明.

$$
\begin{aligned}
\mathcal{D}_R(X) &= \int_G R(e,\hat{g})|\mathcal{F}^{-1}[X](\hat{g}^{-1})|^2 \mu_G(d\hat{g}) \\
&= \int_G R(e,\hat{g}) \left| \sum_{\boldsymbol{\lambda}\in S} \operatorname{Tr} \mathsf{f}_{\boldsymbol{\lambda}}(\hat{g}^{-1}) c_{\boldsymbol{\lambda}} \sqrt{d_{\boldsymbol{\lambda}}} \Phi_{\boldsymbol{\lambda}} \right|^2 \mu_G(d\hat{g}) \\
&= \int_G R(e,\hat{g}) \sum_{\boldsymbol{\lambda},\boldsymbol{\lambda}'\in S} c_{\boldsymbol{\lambda}} c_{\boldsymbol{\lambda}'} \operatorname{Tr} \mathsf{f}_{\boldsymbol{\lambda}^*}(\hat{g}) \otimes \mathsf{f}_{\boldsymbol{\lambda}'}(\hat{g}) \sqrt{d_{\boldsymbol{\lambda}}} \Phi_{\boldsymbol{\lambda}} \otimes \sqrt{d_{\boldsymbol{\lambda}'}} \Phi^\dagger_{\boldsymbol{\lambda}'} \mu_G(d\hat{g}) \\
&= \sum_{\boldsymbol{\lambda},\boldsymbol{\lambda}'\in S} c_{\boldsymbol{\lambda}} c_{\boldsymbol{\lambda}'} \operatorname{Tr} \left[\int_G R(e,\hat{g}) \mathsf{f}_{\boldsymbol{\lambda}^*}(\hat{g}) \otimes \mathsf{f}_{\boldsymbol{\lambda}'}(\hat{g}) \mu_G(d\hat{g}) \right] \sqrt{d_{\boldsymbol{\lambda}}} \Phi_{\boldsymbol{\lambda}} \otimes \sqrt{d_{\boldsymbol{\lambda}'}} \Phi^\dagger_{\boldsymbol{\lambda}'}
\end{aligned}
\tag{4.47}
$$

が成り立つ．ここで，$\Xi_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} := \int_G -R(e,\hat{g}) \mathsf{f}_{\boldsymbol{\lambda}^*}(\hat{g}) \otimes \mathsf{f}_{\boldsymbol{\lambda}'}(\hat{g}) \mu_G(d\hat{g})$ とし，(3.58) を用いると，

$$
\begin{aligned}
\Xi_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} &= \int_G \sum_{\boldsymbol{\lambda}''\in\hat{G}} a_{\boldsymbol{\lambda}''} (\chi_{\boldsymbol{\lambda}''}(\hat{g}) + \chi_{\boldsymbol{\lambda}''^*}(\hat{g})) \mathsf{f}_{\boldsymbol{\lambda}^*}(\hat{g}) \otimes \mathsf{f}_{\boldsymbol{\lambda}'}(\hat{g}) \mu_G(d\hat{g}) \\
&= \sum_{\boldsymbol{\lambda}''\in\hat{G}} a_{\boldsymbol{\lambda}''} \int_G (\chi_{\boldsymbol{\lambda}''}(\hat{g}) + \chi_{\boldsymbol{\lambda}''^*}(\hat{g})) \mathsf{f}_{\boldsymbol{\lambda}^*}(\hat{g}) \otimes \mathsf{f}_{\boldsymbol{\lambda}'}(\hat{g}) \mu_G(d\hat{g}) \\
&= \sum_{\boldsymbol{\lambda}''\in\hat{G}} \frac{a_{\boldsymbol{\lambda}''}}{d_{\boldsymbol{\lambda}''}} (C^{\boldsymbol{\lambda}''^*}_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} I_{\boldsymbol{\lambda}''^*} + C^{\boldsymbol{\lambda}''}_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} I_{\boldsymbol{\lambda}''}) \ge 0
\end{aligned}
$$

が成り立つ．よって，内積 $\langle A,B\rangle := \operatorname{Tr} \Xi_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} A^\dagger B$ に関する Schwarz の不等式を $A := I_{\boldsymbol{\lambda}} \otimes \sqrt{d_{\boldsymbol{\lambda}'}} \Phi_{\boldsymbol{\lambda}'}$, $B := \sqrt{d_{\boldsymbol{\lambda}}} \Phi_{\boldsymbol{\lambda}} \otimes I_{\boldsymbol{\lambda}'}$ に適用すると，

$$
\begin{aligned}
&\operatorname{Tr} \Xi_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} \sqrt{d_{\boldsymbol{\lambda}}} \Phi_{\boldsymbol{\lambda}} \otimes \sqrt{d_{\boldsymbol{\lambda}'}} \Phi^\dagger_{\boldsymbol{\lambda}'} \\
&\quad \le \sqrt{\operatorname{Tr} \Xi_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} d_{\boldsymbol{\lambda}} \Phi^\dagger_{\boldsymbol{\lambda}} \Phi_{\boldsymbol{\lambda}} \otimes I_{\boldsymbol{\lambda}'}} \sqrt{\operatorname{Tr} \Xi_{\boldsymbol{\lambda}^*,\boldsymbol{\lambda}'} I_{\boldsymbol{\lambda}} \otimes d_{\boldsymbol{\lambda}'} \Phi^\dagger_{\boldsymbol{\lambda}'} \Phi_{\boldsymbol{\lambda}'}}
\end{aligned}
$$

$$= \mathrm{Tr}\, \Xi_{\boldsymbol{\lambda}'^*,\boldsymbol{\lambda}}(I_{\boldsymbol{\lambda}'} \otimes I_{\boldsymbol{\lambda}}) = \sum_{\boldsymbol{\lambda}'' \in \hat{G}} a_{\boldsymbol{\lambda}''}(C^{\boldsymbol{\lambda}''^*}_{\boldsymbol{\lambda},\boldsymbol{\lambda}'^*} + C^{\boldsymbol{\lambda}''}_{\boldsymbol{\lambda},\boldsymbol{\lambda}'^*}).$$

この式に，(4.43), (4.47) を組み合わせることで，(4.46) を得る．Schwarz の不等式の等号成立条件より，$X = (c_{\boldsymbol{\lambda}}\Psi_{\boldsymbol{\lambda}})_{\boldsymbol{\lambda}}$ のとき，(4.46) において等号を達成する． □

例 4.3.13 (SU(2)[1, 17, 45]) $G = \mathrm{SU}(2)$ であり，$(\mathbb{C}^2)^{\otimes n}$ への作用が与えられており，自由に参照系を準備できるとする．したがって，表現 f は n が偶数 $2m$ のときは，既約表現 f_λ を重複度 d_λ で含む表現 $\bigoplus_{\lambda=0}^m d_\lambda \mathsf{f}_\lambda$ で与えられ，n が偶数 $2m+1$ のときは，$\bigoplus_{\lambda=0}^m d_{\lambda+\frac{1}{2}} \mathsf{f}_{\lambda+\frac{1}{2}}$ で与えられる．Gate fidelity $\mathcal{R}_{gate}(g) = 1 + \chi_1(g^\dagger \hat{g})$ を利得関数とした場合，

$$C^1_{\lambda,\lambda'} = C^{\lambda'}_{\lambda,1} = \begin{cases} 1 & \text{if } \lambda' = \lambda - 1, \lambda + 1 \\ 0 & \text{上記以外} \end{cases} \tag{4.48}$$

となるので，

$$\mathcal{D}_{\mathcal{R}_{gate}}(\{c_\lambda\}) = \begin{cases} 1 + 2\sum_{\lambda=1}^m c_\lambda c_{\lambda-1} & \text{if } n = 2m \\ 1 + 2\sum_{\lambda=1}^m c_{\lambda+\frac{1}{2}} c_{\lambda-\frac{1}{2}} & \text{if } n = 2m+1 \end{cases} \tag{4.49}$$

となる．定理 4.3.2 より，この値を最大にする $\{c_\lambda\}$ は

$$c_\lambda = \begin{cases} \sin \frac{\lambda+1\pi}{m+2} & \text{if } n = 2m \\ \sin \frac{\lambda+\frac{1}{2}\pi}{m+2} & \text{if } n = 2m+1 \end{cases}$$

であり，最大値は $1 + 2\cos\frac{\pi}{m+2}$ となる．

4.3.6 非コンパクト群の場合*

G が非コンパクト群であり，表現空間 $\mathcal{H} = \bigoplus_{\boldsymbol{\lambda}\in S} \mathcal{U}_{\boldsymbol{\lambda}}$ が無限次元の場合を考える．このとき，任意の初期状態を準備することが物理的に不可能であることが多い．そのため，初期状態にエネルギー拘束を課すことにする [54]．すなわち，$\mathcal{U}_{\boldsymbol{\lambda}}$ 上の半正定値自己共役作用素 $H_{\boldsymbol{\lambda}}$ と定数 E を考え，初期状態 ρ に

条件

$$\mathrm{Tr}\left(\bigoplus_{\boldsymbol{\lambda}\in S} H_{\boldsymbol{\lambda}} \otimes I\right)\rho \le E \tag{4.50}$$

を課す．

この条件は，入力状態が $X \in L^2(\hat{G})$ のとき，

$$\sum_{\boldsymbol{\lambda}\in S} \mathrm{Tr}\, H_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}}^{\dagger} \le E \tag{4.51}$$

となり，以下の定理を得る．

定理 4.3.14　$\boldsymbol{\lambda} \in S$ について $n_{\boldsymbol{\lambda}} = \infty$ とする．このとき，

$$\begin{aligned}&\min_{M,\rho}\{\mathcal{D}_R(M,\rho) \mid (4.50) \text{ を満たす}\}\\ &\quad = \min_{\rho}\{\mathcal{D}_R(M,\rho) \mid (4.50) \text{ を満たす}\}\end{aligned} \tag{4.52}$$

となる．特に，

$$E \min_{X\in L^2(\hat{G})}\left\{\mathcal{D}_R(M_{|I\rangle\langle I|},\rho)\,\middle|\, \sum_{\boldsymbol{\lambda}\in S} \mathrm{Tr}\, H_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}}^{\dagger} \le E \text{ を満たし，} \|X\|_{L^2(\hat{G})} = 1\right\} \tag{4.53}$$

が E に依存しないとき，

$$\begin{aligned}&\min_{\rho}\{\mathcal{D}_R(M,\rho) \mid (4.50) \text{ を満たす}\}\\ &\quad = \min_{X\in L^2(\hat{G})}\left\{\mathcal{D}_R(X)\,\middle|\, \sum_{\boldsymbol{\lambda}\in S} \mathrm{Tr}\, H_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}}^{\dagger} \le E \text{ を満たし，} \|X\|_{L^2(\hat{G})} = 1\right\}\end{aligned} \tag{4.54}$$

を得る．

証明.　最初に，入力状態が純粋状態 $X \in L^2(\hat{G})$ であり，M が $T = \sum_k |\eta_k\rangle\langle\eta_k|$ で与えられる共変的 POVM である場合について考える．このとき，上記の議論と同じ記号を用いると，

$$\sum_{\boldsymbol{\lambda}\in S} \mathrm{Tr}\, H_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}}^{\dagger} = \sum_{\boldsymbol{\lambda}\in S} \sum_k \mathrm{Tr}\, H_{\boldsymbol{\lambda}} X_{\boldsymbol{\lambda}} \eta_k^{\dagger} \eta_k X_{\boldsymbol{\lambda}}^{\dagger}$$

$$= \mathrm{Tr}\left(\bigoplus_{\boldsymbol{\lambda}\in S} H_{\boldsymbol{\lambda}} \otimes I\right)\left(\sum_k |x_k\rangle\langle x_k|\right).$$

したがって，混合状態 $\sum_k |x_k\rangle\langle x_k|$ を初期状態とし，T を $|I\rangle\langle I|$ とする共変的測定で測った場合のコストと一致する．次に，確率的に $X \in L^2(\hat{G})$ を選んだ場合を考える．この場合，個々の X に対して $\sum_k |x_k\rangle\langle x_k|$ を上記の手続きで決定し，それらを確率的に重ね合わせた状態を入力状態とした場合に帰着できる．したがって，(4.52) を得る．

そして，(4.53) が E に依存しない定数 C のとき，(4.52) の右辺は，

$$\inf\left\{\sum_i p_i \frac{C}{E_i} \,\middle|\, \sum_i p_i E_i = E\right\} \tag{4.55}$$

となる．ベクトル $(\sqrt{p_i E_i})$, $\left(\sqrt{\frac{Cp_i}{E_i}}\right)$ についての Schwartz の不等式より，$\sum_i p_i \frac{C}{E_i} \sum_i p_i E_i \le \sum_i p_i C = C$ となることから，上記の値は $\frac{C}{E}$ となり，(4.54) を得る．□

例 4.3.15（Heisenberg 表現）$\mathbb{R}^2$ の Heisenberg 表現 W（[37] の 6.1.1 項を参照）では表現空間が無限次元となるため，定理 4.3.14 で扱ったように，エネルギー拘束を課すことが自然である．$L^2(\mathbb{R})$ を表現空間とし，その重複度を表す空間も $L^2(\mathbb{R})$ とすると，入力状態は $L^2(\mathbb{R})^{\otimes 2}$ 上の純粋状態 $|X\rangle\rangle$ として与えられる．このとき，真のパラメータからの差の二乗で誤差を測ると，誤差は以下で与えられる．

$$\int_{\mathbb{R}^2} (x^2+y^2)|\mathcal{F}^{-1}[X](-\zeta)|^2 dxdy. \tag{4.56}$$

ここで，$\zeta = \frac{x+iy}{\sqrt{2}}$ とした．以下のエネルギー拘束条件を考える．

$$\langle\langle X|Q^2+P^2|X\rangle\rangle \le E. \tag{4.57}$$

そして，(4.56) は [37] の (6.59) に一致し，(4.57) は [37] の (6.58) に一致するので，[37] の 6.7 節の議論より，条件 (4.57) の下での (4.56) の最小値は $\frac{1}{2E}$ となる．

4.4 通信路と対称性

次に，量子通信路が対称性を満たす場合について扱う．2つの量子系 $\mathcal{H}_1, \mathcal{H}_2$ が与えられ，それぞれに対して群 G の射影的ユニタリ表現 $\mathsf{f}_1, \mathsf{f}_2$ が与えられたとする．そして，量子系 $\mathcal{H}_1$ から量子系 $\mathcal{H}_2$ への量子通信路 Λ が以下の条件を満たすとき，$\mathsf{f}_1, \mathsf{f}_2$ について**共変的**であるという．

$$\Lambda(\mathsf{f}_1(g)\rho\mathsf{f}_1(g)^\dagger) = \mathsf{f}_2(g)\Lambda(\rho)\mathsf{f}_2(g)^\dagger, \quad \forall g \in G. \tag{4.58}$$

そして，共変的な量子通信路の集合を $\mathcal{T}_{\mathrm{cov}}(\mathsf{f}_1, \mathsf{f}_2)$ と記す．この条件は Λ の Choi-Jamiolkowski 表現 $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ に対する以下の条件を同値である．

$$\begin{aligned}
&(\mathsf{f}_2(g) \otimes \overline{\mathsf{f}_1}(g))^{-1}(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)(\mathsf{f}_2(g) \otimes \overline{\mathsf{f}_1}(g)) \\
&= (\mathsf{f}_2(g)^\dagger \otimes \mathsf{f}_1(g)^T)(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)(\mathsf{f}_2(g) \otimes \overline{\mathsf{f}_1}(g)) \\
&= (\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|), \quad \forall g \in G.
\end{aligned} \tag{4.59}$$

$\mathcal{H}_1$ の参照系を $\mathcal{H}_{1,R}$ とすると，したがって，$(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ は $\mathcal{H}_2 \otimes \mathcal{H}_{1,R}$ 上の表現 $\mathsf{f}_2 \otimes \overline{\mathsf{f}_1}$ の下で不変となる．表現空間 $\mathcal{H}_2 \otimes \mathcal{H}_{1,R}$ の既約分解を $\bigoplus_{\boldsymbol{\lambda} \in S} \mathcal{U}_{\boldsymbol{\lambda}} \otimes \mathbb{C}^{m_{\boldsymbol{\lambda}}}$ とすると，Schur の補題から $(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)$ の形は，$\bigoplus_{\boldsymbol{\lambda} \in S} I_{\boldsymbol{\lambda}} \otimes T_{\boldsymbol{\lambda}}$ と書ける．ただし，$T_{\boldsymbol{\lambda}}$ は $\mathbb{C}^{m_{\boldsymbol{\lambda}}}$ 上の半正定値行列である．

なお，表現 $\mathsf{f}_2 \otimes \overline{\mathsf{f}_1}$ の表現空間は $\mathcal{H}_1$ から $\mathcal{H}_2$ への線形写像のなす空間（行列空間）と考えることができる．ここで，以下の補題が成り立つ．

補題 4.4.1　$\mathsf{f}_1, \mathsf{f}_2$ を群 G の $\mathcal{H}_1, \mathcal{H}_2$ 上の既約な射影的ユニタリ表現とする．系 $\mathcal{H}_1$ から系 $\mathcal{H}_2$ への完全性写像 Λ は $\mathsf{f}_1, \mathsf{f}_2$ について共変的であるとする．このとき完全性写像 Λ がトレースを保存する（量子通信路である）ための必要十分条件は以下を満たすことである．

$$\Lambda(I_{\mathcal{H}_1}) = \frac{\dim \mathcal{H}_1}{\dim \mathcal{H}_2} I_{\mathcal{H}_2}. \tag{4.60}$$

群 G が非コンパクトである場合には形式的次元 $\dim \mathcal{H}_1, \dim \mathcal{H}_2$ が存在するときにこの事実は成り立つ．なお，形式的次元 $\dim \mathcal{H}_1$ が存在せず，形式的次元 $\dim \mathcal{H}_2$ のみが存在するときは，共変的な量子通信路は存在しない．

証明.　$\frac{1}{\dim \mathcal{H}_1} I_{\mathcal{H}_1} = \int_G \mathsf{f}_1(g)\rho\mathsf{f}_1(g)^\dagger \mu_G(dg)$ であるため，Λ の共変的より

$$\Lambda\left(\int_G \mathsf{f}_1(g)\rho\mathsf{f}_1(g)^\dagger\mu_G(dg)\right) = \int_G \mathsf{f}_2(g)\Lambda(\rho)\mathsf{f}_2(g)^\dagger\mu_G(dg) = \frac{\operatorname{Tr}\Lambda(\rho)}{\dim\mathcal{H}_2}I_{\mathcal{H}_2}$$

となる．Λ がトレースを保存するとき，$\operatorname{Tr}\Lambda(\rho)=1$ となり，(4.60) が成り立つ．逆に，(4.60) が成り立つとき，$\operatorname{Tr}\Lambda(\rho)=1$ となり，Λ はトレースを保存する．

形式的次元 $\dim\mathcal{H}_1$ が存在せず，形式的次元 $\dim\mathcal{H}_2$ のみが存在するときは，双対写像を Λ^* とし，ρ' を $\mathcal{H}_2$ 上の状態とすると，

$$\begin{aligned}\operatorname{Tr}\rho'\frac{1}{\dim\mathcal{H}_2}I_{\mathcal{H}_2} &= \operatorname{Tr}\rho'\Lambda\left(\int_G \mathsf{f}_1(g)\rho\mathsf{f}_1(g)^\dagger\mu_G(dg)\right)\\ &= \operatorname{Tr}\Lambda^*(\rho')\int_G \mathsf{f}_1(g)\rho\mathsf{f}_1(g)^\dagger\mu_G(dg)\end{aligned}$$

となる．右辺は発散するが，左辺は発散しない値であるため，矛盾が生じる．よって，共変的な量子通信路は存在しない．　□

量子系 $\mathcal{H}_1$ に群 G の射影的ユニタリ表現 f_1 が与えられたとする．G 上の確率分布 ν に対して，$\mathcal{H}_1$ を入出力系とする量子通信路 $\Lambda[\mathsf{f}_1,\nu]$ を $\Lambda[\mathsf{f}_1,\nu](\rho) := \int_G \mathsf{f}_1(g)\rho\mathsf{f}_1(g)^\dagger\nu(dg)$ で定義する．このとき，量子通信路 $\Lambda[\mathsf{f}_1,\nu]$ の Choi-Jamiolkowski 表現は

$$\sum_{g\in G}\nu(g)|\mathsf{f}_1(g)\rangle\rangle\langle\langle\mathsf{f}_1(g)| \tag{4.61}$$

となる．逆に，Choi-Jamiolkowski 表現が (4.61) で与えられる量子通信路は $\Lambda[\mathsf{f}_1,\nu]$ となる．

さらに，もう 1 つの量子系 $\mathcal{H}_2$ に対しても群 G の射影的ユニタリ表現 f_2 が与えられたとし，量子系 $\mathcal{H}_1$ から $\mathcal{H}_2$ への量子通信路 Λ が与えられたとする．このとき，G 上の確率分布 ν についての Λ の**平均化通信路** $\overline{\Lambda}_\nu$ を以下で定義する．

$$\overline{\Lambda}_\nu(\rho) := \int_G \mathsf{f}_2(g)^{-1}\Lambda(\mathsf{f}_1(g)\rho\mathsf{f}_1(g)^{-1})\mathsf{f}_2(g)\nu(dg). \tag{4.62}$$

特に，ν が コンパクト Lie 群 G の不変測度 μ である場合，$\overline{\Lambda}_\mu$ は G の射影的ユニタリ表現 $\mathsf{f}_1,\mathsf{f}_2$ についての Λ の **twirling** とよばれる．f_2 が f_1 と等し

いときは，単に，$\overline{\Lambda}_\mu$ は G の射影的ユニタリ表現 f_1 についての Λ の twirling とよばれる．

定理 4.4.2　Λ を量子系 $\mathcal{H}_1$ から量子系 $\mathcal{H}_2$ への量子通信路（完全正写像）とし，$\mathsf{f}_1, \mathsf{f}_2$ をそれぞれの空間上のコンパクト Lie 群 G 射影的ユニタリ表現とする．$\mathsf{f}_1, \mathsf{f}_2$ についての Λ の twirling $\overline{\Lambda}_\mu$ は $\mathsf{f}_1, \mathsf{f}_2$ について共変的である．

系 4.4.3　定理 4.4.2 と同じ条件の下で，G 上の測度 ν が $\mathsf{f}_2 \otimes \overline{\mathsf{f}_1}$-design とする．このとき，$\nu$ についての Λ の平均化通信路 $\overline{\Lambda}_\nu$ は $\mathsf{f}_1, \mathsf{f}_2$ について共変的である．

例 4.4.4　(Pauli 通信路)　$\mathbb{X}$ が $\mathbb{Z}_d$ または $\mathbb{F}_q$ であり，入出力系に群 $\mathbb{X}^{2r}$ の離散 Heisenberg 表現 $\mathsf{W}^r_{\mathbb{X}}$ が与えられた場合に共変的な量子通信路は **Pauli 通信路**とよばれる．表現 $\mathsf{W}^r_{\mathbb{X}} \otimes \overline{\mathsf{W}^r_{\mathbb{X}}}$ の既約成分は，1 次元となる．この表現の表現空間を行列空間として考えた場合，1 次元の既約成分を与える基底は $\vec{s} \in \mathbb{X}^{2r}$ を用いて $\mathsf{W}^r_{\mathbb{X}}(\vec{s})$ と表せる．この場合，$\mathbb{X}^{2r}$ 上の確率分布 P を用いると，通信路の Choi-Jamiolkowski 表現は $\sum_{\vec{s} \in \mathbb{X}^{2r}} \mathrm{P}(\vec{s}) |\mathsf{W}^r_{\mathbb{X}}(\vec{s})\rangle\rangle\langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s})|$ となる．したがって，対応する Pauli 通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}]$ は

$$\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}](\rho) = \sum_{\vec{s} \in \mathbb{X}^{2r}} \mathrm{P}(\vec{s}) \mathsf{W}^r_{\mathbb{X}}(\vec{s}) \rho \mathsf{W}^r_{\mathbb{X}}(\vec{s})^\dagger \tag{4.63}$$

と表せる．一般の量子通信路 Λ に対して，

$$P[\Lambda](\vec{s}) := \frac{1}{|\mathbb{X}^r|^2} \langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s}) | \Lambda \otimes id(|I\rangle\rangle\langle\langle I|) | \mathsf{W}^r_{\mathbb{X}}(\vec{s})\rangle\rangle \tag{4.64}$$

とすると，Λ の離散 Heisenberg 表現 $\mathsf{W}^r_{\mathbb{X}}$ についての twirling は $\Lambda[\mathsf{W}^r_{\mathbb{X}}, P[\Lambda]]$ と一致する [5, 28]．この事実は両者の Choi-Jamiolkowski 表現を比較するとすぐに確認できる．

例 4.4.5　(Depolarizing 通信路)　入出力系に群 $\mathrm{SU}(r)$ の基本表現 $\mathsf{f}_{[1,0,\ldots,0]}$ が与えられた場合に共変的な量子通信路は **Depolarizing 通信路**とよばれる．$\mathsf{f}_{[1,0,\ldots,0]} \otimes \overline{\mathsf{f}_{[1,0,\ldots,0]}}$ の表現空間を $\mathbb{C}^r$ 上の行列空間として考えた場合，既約成分は，単位行列からなる 1 次元の既約成分とその直交補空間からなる既約成分に分かれる．したがって，実数 $t \geq 0$ を用いて，通信路の Choi-Jamiolkowski

表現は $t|I\rangle\rangle\langle\langle I| + \frac{(1-t)}{r}I$ と表せる．したがって，対応する Depolarizing 通信路 $\Lambda_{\mathsf{f}_{[1,0,\ldots,0]},t}$ は $\Lambda_{\mathsf{f}_{[1,0,\ldots,0]},t}(\rho) = t\rho + (1-t)\rho_{\mathrm{mix}}$ と表せる．

特に，$\mathrm{SU}(r)$ 上の測度 ν が Λ が $\mathbb{C}^r$ から $\mathbb{C}^r$ への量子通信路であるとき，$(2,0)$-design となるとき，ν についての平均化量子通信路 $\overline{\Lambda}_\nu$ は Depolarizing 通信路となる．

例 4.4.6 （共役 Depolarizing 通信路） 入力系に群 $\mathrm{SU}(r)$ の基本表現 $\mathsf{f}_{[1,0,\ldots,0]}$ が与えられ，出力系にその複素共役表現 $\overline{\mathsf{f}_{[1,0,\ldots,0]}} = \mathsf{f}_{[0,\ldots,0,1]}$ が与えられた場合，共変的な量子通信路は**共役 Depolarizing 通信路**とよぶ．

$\overline{\mathsf{f}_{[1,0,\ldots,0]}} \otimes \overline{\mathsf{f}_{[1,0,\ldots,0]}} = \mathsf{f}_{[0,\ldots,0,1]}^{\otimes 2}$ の表現空間は対称テンソル積空間 $\mathcal{H}_s$ と反対称テンソル積空間 $\mathcal{H}_a$ に既約分解できる．したがって，実数 $t \geq 0$ を用いて，通信路の Choi-Jamiolkowski 表現は $\frac{1+(r-1)t}{r}P_s + \frac{1-(r+1)t}{r}P_a$ と表せる．ここで，P_s, P_a は $\mathcal{H}_s, \mathcal{H}_a$ への射影である．

例えば，転置を与える作用 $\rho \mapsto \rho^T$ の Choi-Jamiolkowski 表現は $P_s - P_a$ となる．したがって，対応する共役 Depolarizing 通信路 $\Lambda_{[1,0,\ldots,0]\to[0,\ldots,0,1],t}$ は

$$\Lambda_{[1,0,\ldots,0]\to[0,\ldots,0,1],t}(\rho) = t\rho^T + (1-t)\rho_{\mathrm{mix}} \tag{4.65}$$

と表せる．したがって，補題 2.1.1 より，共役 Depolarizing 通信路が完全正写像となるための必要十分条件は $-\frac{1}{r-1} \leq t \leq \frac{1}{r+1}$ で与えられる．

以下，群 G の既約表現 $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \boldsymbol{\lambda}_3 \in \hat{G}$ が与えられ，$\mathcal{U}_{\boldsymbol{\lambda}_1} \otimes \mathcal{U}_{\boldsymbol{\lambda}_3}$ の既約成分に $\mathcal{U}_{\boldsymbol{\lambda}_2}$ が重複度 1 で含まれるとする．このとき，$P_{\boldsymbol{\lambda}_2}$ を $\mathcal{U}_{\boldsymbol{\lambda}_2}$ への射影とし，$d_{\boldsymbol{\lambda}_1}, d_{\boldsymbol{\lambda}_2}$ は表現空間 $\mathcal{U}_{\boldsymbol{\lambda}_1}, \mathcal{U}_{\boldsymbol{\lambda}_2}$ の次元とすると，[37] の (3.53) より，

$$\mathrm{Tr}\, P_{\boldsymbol{\lambda}_2}(\rho \otimes I_{\mathcal{U}_{\boldsymbol{\lambda}_3}})P_{\boldsymbol{\lambda}_2}\frac{d_{\boldsymbol{\lambda}_2}}{d_{\boldsymbol{\lambda}_1}} \tag{4.66}$$

を得る．なお，G が非コンパクト群の場合は形式的次元を表すとする．したがって，以下の量子通信路 $\Lambda^+_{\boldsymbol{\lambda}_1\to\boldsymbol{\lambda}_2}$ （$\boldsymbol{\lambda}_1 \to \boldsymbol{\lambda}_2$ の**拡大共変量子通信路**とよぶ）が定義できる．

$$\Lambda^+_{\boldsymbol{\lambda}_1\to\boldsymbol{\lambda}_2}(\rho) := \frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}}P_{\boldsymbol{\lambda}_2}(\rho \otimes I_{\mathcal{U}_{\boldsymbol{\lambda}_3}})P_{\boldsymbol{\lambda}_2}. \tag{4.67}$$

$\mathcal{U}_{\boldsymbol{\lambda}_1^*} \otimes \mathcal{U}_{\boldsymbol{\lambda}_2}$ は重複度 1 で $\mathcal{U}_{\boldsymbol{\lambda}_3}$ を含む（[37, 補題 2.7.3] 参照）．したがって，量子通信路 $\Lambda^+_{\boldsymbol{\lambda}_1 \to \boldsymbol{\lambda}_2}$ の Choi-Jamiolkowski 表現は $\mathcal{U}_{\boldsymbol{\lambda}_3}$ 上の射影の定数倍となる（[37, 補題 2.7.4 の **(1)**] 参照）．

さらに，$\Lambda^-_{\boldsymbol{\lambda}_2 \to \boldsymbol{\lambda}_1}(\rho) := \mathrm{Tr}_{\mathcal{U}_{\boldsymbol{\lambda}_3}} \rho$ で定義できる量子通信路 $\Lambda^-_{\boldsymbol{\lambda}_2 \to \boldsymbol{\lambda}_1}$ を $\boldsymbol{\lambda}_2 \to \boldsymbol{\lambda}_3$ の**縮小共変量子通信路**とよぶ．ここで，ρ を $\mathcal{U}_{\boldsymbol{\lambda}_1} \otimes \mathcal{U}_{\boldsymbol{\lambda}_3}$ 上の密度行列と見なして部分トレース $\mathrm{Tr}_{\mathcal{U}_{\boldsymbol{\lambda}_3}}$ をとった．すると，[37] の補題 2.7.4 の **(1)** より，量子通信路 $\Lambda^-_{\boldsymbol{\lambda}_2 \to \boldsymbol{\lambda}_1}$ の Choi-Jamiolkowski 表現は $\mathcal{U}_{\boldsymbol{\lambda}_3^*}$ 上の射影の定数倍となる．

4.5　近似的状態複製

4.1 節では，群 G の $\mathcal{H}$ への（射影的）ユニタリ表現 f と，$\mathcal{H}$ 上の f に関して共変的な状態族 $\{\rho_\theta\}_{\theta\in\Theta}$ が与えられたときに，測定の最適化を扱った．本節では，同じ群 G の $\mathcal{H}_1$ への（射影的）ユニタリ表現 f_1 と，$\mathcal{S}(\mathcal{H}_1)$ 上の関数族 $\{R_\theta\}_{\theta\in\Theta}$ が与えられたときに，系 $\mathcal{H}$ から系 $\mathcal{H}_1$ への状態操作 Λ に関して最適化を行う．数学的には状態操作は量子通信路そのものであるが，本節では，状態変化を最適化するので，状態操作という表現を用いることにする．

真のパラメータが θ であったときの状態操作 Λ の性能 $R_\theta(\Lambda(\rho_\theta))$ を定義し，この値を大きくする Λ を選ぶ問題を考える．この問題は後に述べる近似的状態複製を含む一般的な設定である．パラメータ θ は未知であるので，θ についての最悪値 $R(\Lambda) := \max_\Lambda R_\theta(\Lambda(\rho_\theta))$ を最適化する方法や，θ についての分布 ν の下での平均値 $R_\nu(\Lambda) := \int_\Theta R_\theta(\Lambda(\rho_\theta))\nu(d\theta)$ を最適化する方法がある．

一般的な設定の下でこの問題を扱うことは困難であるので，以下では，$\mathcal{S}(\mathcal{H}_1)$ 上の関数族 $\{R_\theta\}_{\theta\in\Theta}$ が表現 f_1 に関して**共変性条件** $R_\theta(\mathsf{f}_1(g)^\dagger \rho \mathsf{f}_1(g)) = R_{g\theta}(\rho)$ を課す．

このとき，定理 4.1.1 の証明と同じように，(4.62) で定義した平均化通信路を用いて，以下の定理を示すことができる．

定理 4.5.1　Θ はコンパクトであり，関数族 $\{R_\theta\}_{\theta\in\Theta}$ が表現 f_1 に関する共変性条件を満たし，各関数 R_θ は凸関数であるとする．このとき以下が成り立つ．

$$\min_{\Lambda\in\mathcal{T}(\mathcal{H},\mathcal{H}_1)} R(\Lambda) = \min_{\Lambda\in\mathcal{T}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda) = \min_{\Lambda\in\mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)} R(\Lambda)$$

$$= \min_{\Lambda \in \mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda).$$

$\mathcal{T}(\mathcal{H},\mathcal{H}_1)$ ($\mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)$) は系 $\mathcal{H}$ から $\mathcal{H}_1$ への（共変的） TP-CP 写像の集合である．すなわち，mini-max 法の解と，不変測度 μ による Bayes 法の最適値は一致し，最適な状態操作は共変的な状態操作で与えられる．また，mini-max 法の解を与える状態操作は共変的である．

証明.　任意の Λ は $R_\theta(\mathsf{f}_1(g)^\dagger\Lambda(\mathsf{f}(g)\rho_\theta\mathsf{f}(g)^\dagger)\mathsf{f}_1(g)) = R_{g\theta}\Lambda(\rho_{g\theta})$ を満たす．したがって，R_θ の凸性より，

$$\int_G R_{g\theta}\Lambda(\rho_{g\theta})\mu(dg) = \int_G R_\theta(\mathsf{f}_1(g)^\dagger\Lambda(\mathsf{f}(g)\rho_\theta\mathsf{f}(g)^\dagger)\mathsf{f}_1(g))\mu(dg)$$
$$\geq R_\theta\left(\int_G \mathsf{f}_1(g)^\dagger\Lambda(\mathsf{f}(g)\rho_\theta\mathsf{f}(g)^\dagger)\mathsf{f}_1(g)\mu(dg)\right) = R_\theta\left(\int_G \overline{\Lambda}_\mu(\rho_\theta)\right)$$

が成り立つ．$\overline{\Lambda}_\mu$ は共変的な TP-CP 写像であるので，

$$\min_{\Lambda \in \mathcal{T}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda) \geq \min_{\Lambda \in \mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda) = \min_{\Lambda \in \mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda)$$

を得る．逆方向の不等式，

$$\min_{\Lambda \in \mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda) \geq \min_{\Lambda \in \mathcal{T}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda) \geq \min_{\Lambda \in \mathcal{T}(\mathcal{H},\mathcal{H}_1)} R_{\mu_\Theta}(\Lambda)$$

が成り立つことから題意を得る．　□

Θ がコンパクトでない場合は，不変測度 μ の積分が有限値ではないので，上記の定理は Bayes 法については成立しないが，定理 4.1.1 と同様に，mini-max 法について以下の定理が成立する．

定理 4.5.2　Θ は局所コンパクトであるとする．共変的な状態操作 Λ に対して $R(\Lambda) = R_\theta(\Lambda(\rho_\theta))$ が成り立つ．

さらに，$\min_{\Lambda \in \mathcal{T}(\mathcal{H},\mathcal{H}_1)} R(\Lambda) = \min_{\Lambda \in \mathcal{T}_{\mathrm{cov}}(\mathcal{H},\mathcal{H}_1)} R(\Lambda)$ が成り立つ．

以下，状態操作の最適化の具体例として，**量子状態の近似的複製**を扱う．近似的複製とは，ある状態 ρ の複製が n 個与えられたとき，状態は $\rho^{\otimes n}$ で与えられ，n 個から $n+m$ 個の複製となる状態 $\rho^{\otimes(n+m)}$ を生成する問題である．候補

となる状態 ρ が限られており，それらが完全に識別できる場合には，完全な複製が可能であるが，それ以外の場合には不可能である．そのため，近似的に状態 $\rho^{\otimes(n+m)}$ を生成する問題を扱うことにする．群 G の系 $\mathcal{H}'$ 上への表現 f' に関して共変な状態族 $\{\rho'_\theta\}_{\theta\in\Theta}$ が与えられたとき，系 $\mathcal{H}$ 上の $\{\rho_\theta\}_{\theta\in\Theta}$ の状態族を $\{\rho'^{\otimes n}_\theta\}_{\theta\in\Theta}$ とし，状態操作 Λ の性能を $R_\theta(\Lambda(\rho'^{\otimes n}_\theta)) = \mathrm{Tr}\,\Lambda(\rho'^{\otimes n}_\theta)\rho'^{\otimes(n+m)}_\theta$ で測ることにする．この場合，$R_\theta(\Lambda(\rho'^{\otimes n}_\theta))$ の最大化を考えることになる．近似的複製とは，群共変的な設定での状態操作の最適化の特殊例となり，定理 4.5.1, 4.5.2 を適用することができる．このように，近似的状態複製の問題は上記の群共変的な設定での状態操作の最適化の枠組みで扱うことができる．

ρ_θ が純粋状態からなる共変的状態族の近似的複製を一般化した問題について以下の補題が成り立つ．

補題 4.5.3　群 G の既約ユニタリ表現 $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \hat{G}$ について純粋状態からなる同じパラメータを持つ共変的状態族 $\{\rho_{1,\theta}\}_{\theta\in\Theta}$，$\{\rho_{2,\theta}\}_{\theta\in\Theta}$ の下で，$R_\theta(\Lambda(\rho_{1,\theta})) := \mathrm{Tr}\,\Lambda(\rho_{1,\theta})\rho_{2,\theta}$ を与える．このとき，

$$\min_{\Lambda\in\mathcal{T}_{\mathrm{cov}}(\mathsf{f}_{\boldsymbol{\lambda}_1},\mathsf{f}_{\boldsymbol{\lambda}_2})} R(\Lambda) \le \frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}} \tag{4.68}$$

を得る．

証明.　Λ を共変的量子通信路とする．補題 4.4.1 より，

$$\mathrm{Tr}\,\Lambda(\rho_{1,\theta})\rho_{2,\theta} \le \mathrm{Tr}\,\Lambda(I)\rho_{2,\theta} = \mathrm{Tr}\,\frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}} I\rho_{2,\theta} = \frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}} \tag{4.69}$$

となり題意を得る．　□

群 G の既約ユニタリ表現 $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \hat{G}$ について純粋状態からなる同じパラメータを持つ共変的状態族 $\{\rho_{1,\theta}\}_{\theta\in\Theta}$, $\{\rho_{2,\theta}\}_{\theta\in\Theta}$ に対して，以下の条件を満たす群 G の既約ユニタリ表現 $\boldsymbol{\lambda}_3 \in \hat{G}$ と同じパラメータを持つ $\mathsf{f}_{\boldsymbol{\lambda}_3}$ について共変的な状態族 $\{\rho_{3,\theta}\}_{\theta\in\Theta}$ が存在するとき，$\{\rho_{2,\theta}\}_{\theta\in\Theta}$ は $\{\rho_{1,\theta}\}_{\theta\in\Theta}$ の**拡大共変的状態族**とよぶことにする．$\mathcal{U}_{\boldsymbol{\lambda}_1} \otimes \mathcal{U}_{\boldsymbol{\lambda}_3}$ に既約表現 $\mathcal{U}_{\boldsymbol{\lambda}_2}$ が重複度 1 で含まれ，$\rho_{1,\theta} \otimes \rho_{3,\theta} = \rho_{2,\theta}$ を満たす．

補題 4.5.4　補題 4.5.3 の仮定に加え，$\{\rho_{2,\theta}\}_{\theta\in\Theta}$ が $\{\rho_{1,\theta}\}_{\theta\in\Theta}$ の拡大共変的状態族であるとき，$\boldsymbol{\lambda}_1 \to \boldsymbol{\lambda}_2$ の拡大共変量子通信路 $\Lambda^{+}_{\boldsymbol{\lambda}_1\to\boldsymbol{\lambda}_2}$ は

$$R(\Lambda^+_{\boldsymbol{\lambda}_1\to\boldsymbol{\lambda}_2}) = \frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}} \tag{4.70}$$

を満たす．すなわち，(4.68) において等号が成り立つ．したがって，$\Lambda_{\boldsymbol{\lambda}_1+\boldsymbol{\lambda}_3=\boldsymbol{\lambda}_2}$ は最適性能を実現する．

証明.

$$\begin{aligned}\operatorname{Tr}\Lambda^+_{\boldsymbol{\lambda}_1\to\boldsymbol{\lambda}_2}(\rho_{1,\theta})\rho_{2,\theta} &= \operatorname{Tr}\frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}}Q_{\boldsymbol{\lambda}_2}(\rho_{1,\theta}\otimes I_{\mathcal{U}_{\boldsymbol{\lambda}_3}})Q_{\boldsymbol{\lambda}_2}\rho_{2,\theta}\\ &\geq \operatorname{Tr}\frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}}Q_{\boldsymbol{\lambda}_2}(\rho_{1,\theta}\otimes\rho_{3,\theta})Q_{\boldsymbol{\lambda}_2}\rho_{2,\theta} = \frac{d_{\boldsymbol{\lambda}_1}}{d_{\boldsymbol{\lambda}_2}}\end{aligned}$$

となる．逆向きの不等式は (4.68) より保証されるので題意を得る． □

例えば，G が Lie 群であり，現れる既約表現 $\mathsf{f}_{\boldsymbol{\lambda}_1}$ が最高ウェイト $\boldsymbol{\lambda}_1$ によって決まる表現であり，$\mathsf{f}_{\boldsymbol{\lambda}_3}$ が $\boldsymbol{\lambda}_1$ のスカラー倍の最高ウェイト $\boldsymbol{\lambda}_3$ によって与えられる場合を考えよう．$\boldsymbol{\lambda}_2=\boldsymbol{\lambda}_1+\boldsymbol{\lambda}_3$ とすると，共変的状態族 $\{\rho_{2,\theta}\}_{\theta\in\Theta}$ $\{\rho_{1,\theta}\}_{\theta\in\Theta}$ を コヒーレント状態族とすると $\{\rho_{2,\theta}\}_{\theta\in\Theta}$ は $\{\rho_{1,\theta}\}_{\theta\in\Theta}$ の拡大共変的状態族となる．特に，$\boldsymbol{\lambda}_1$, $\boldsymbol{\lambda}_3$ があるウェイト $\boldsymbol{\lambda}$ の整数 n, m 倍で与えられる場合は n 個のコヒーレント状態を $n+m$ 個のコヒーレント状態に複製する問題となる．

このように整数倍で与えられる場合については，状態操作 Λ の評価の基準として，

$$\operatorname{Tr}\rho_{1,\theta}\frac{1}{n+m}\sum_{j=1}^{n+m}(\operatorname{Tr}_{\check{j}}\Lambda(\rho_{1,\theta}^{\otimes n})) = \operatorname{Tr}\mathcal{E}(\rho_{1,\theta}^{\otimes n})\frac{1}{n+m}\sum_{j=1}^{n+m}\rho_{1,\theta}^{(j)}$$

が用いられることもある．この基準では，各系に注目したときの状態とターゲットとなる状態 $\rho_{1,\theta}$ との近さの平均値を問題にしている．補題 4.5.4 で最適性が示された状態操作 $\Lambda^+_{n\boldsymbol{\lambda}\to(n+m)\boldsymbol{\lambda}}$ を用いたとき，この基準の下での性能は以下のように計算できる．以下の計算では，$P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}}$ と $\frac{1}{n+m}\sum_{j=1}^{n+m}\rho_{1,\theta}^{(j)}$ が交換可能であることに注目する．

$$\begin{aligned}&\operatorname{Tr}\Lambda^+_{n\boldsymbol{\lambda}\to(n+m)\boldsymbol{\lambda}}(\rho_{1,\theta}^{\otimes n})\frac{1}{n+m}\sum_{j=1}^{n+m}\rho_{1,\theta}^{(j)}\\ &= \frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}}\operatorname{Tr}P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}}\rho_{1,\theta}^{\otimes n}\otimes I_{\boldsymbol{\lambda}}^{\otimes m}P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}}\frac{1}{n+m}\sum_{j=1}^{n+m}\rho_{1,\theta}^{(j)}\end{aligned}$$

$$
\begin{aligned}
&= \frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}} \operatorname{Tr} P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}} \rho_{1,\theta}^{\otimes n} \otimes I_{\boldsymbol{\lambda}}^{\otimes m} \frac{1}{n+m} \sum_{j=1}^{n+m} \rho_{1,\theta}^{(j)} \\
&= \frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}} \frac{1}{n+m} \sum_{j=1}^{n+m} \operatorname{Tr} P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}} \rho_{1,\theta}^{(j)} \rho_{1,\theta}^{\otimes n} \otimes I_{\boldsymbol{\lambda}}^{\otimes m} \\
&= \frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}} \left(\frac{n}{n+m} \frac{d_{(n+m)\boldsymbol{\lambda}}}{d_{n\boldsymbol{\lambda}}} + \frac{m}{m+n} \frac{d_{(n+m)\boldsymbol{\lambda}}}{d_{(n+1)\boldsymbol{\lambda}}} \right) \qquad (4.71) \\
&= \frac{n}{n+m} + \frac{m}{n+m} \frac{d_{n\boldsymbol{\lambda}}}{d_{(n+1)\boldsymbol{\lambda}}} = 1 - \frac{m}{n+m} \frac{d_{(n+1)\boldsymbol{\lambda}} - d_{n\boldsymbol{\lambda}}}{d_{(n+1)\boldsymbol{\lambda}}}.
\end{aligned}
$$

(4.71) では，(4.66) を用いて得られる以下の事実を用いた．

$$
\begin{aligned}
&\operatorname{Tr} P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}} \rho_{1,\theta}^{(j)} \rho_{1,\theta}^{\otimes n} \otimes I_{\boldsymbol{\lambda}}^{\otimes m} \\
&= \begin{cases} \operatorname{Tr} P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}} \rho_{1,\theta}^{\otimes n} \otimes I_{\boldsymbol{\lambda}}^{\otimes m} = \frac{d_{(n+m)\boldsymbol{\lambda}}}{d_{n\boldsymbol{\lambda}}} & 1 \le j \le n \text{ のとき} \\ \operatorname{Tr} P_{\mathcal{U}_{(n+m)\boldsymbol{\lambda}}} \rho_{1,\theta}^{\otimes n+1} \otimes I_{\boldsymbol{\lambda}}^{\otimes (m-1)} = \frac{d_{(n+m)\boldsymbol{\lambda}}}{d_{(n+1)\boldsymbol{\lambda}}} & n+1 \le j \le n+m \text{ のとき．} \end{cases}
\end{aligned}
$$

すなわち，この基準の下での複製の精度は n 個の複製があるときの推定精度 $\frac{d_{n\boldsymbol{\lambda}}}{d_{(n+1)\boldsymbol{\lambda}}}$ と比率 $\frac{n}{n+m}$ の関数として得られる．特に，要求される複製の数 $n+m$ について無限大の極限を考えると，そのときの精度の値は，n 個の複製があるときの推定精度 $\frac{d_{n\boldsymbol{\lambda}}}{d_{(n+1)\boldsymbol{\lambda}}}$ と一致する．

なお，Lie 群の場合，射影的ユニタリ表現を考えることがあるが，有限次元の場合は，対応する Lie 環の歪エルミート表現に対応することが多い．以下の例では，Lie 環の歪エルミート表現を考えるが，不変被覆群のユニタリ表現を考えているとする．

例 4.5.5　($\mathfrak{su}(2)$[23, 115]$\mathfrak{su}(1,1)$)　$\mathfrak{g} = \mathfrak{su}(2), \mathfrak{su}(1,1)$ の場合は，λ は $\lambda < 0$ の実数か正の半整数に限られる．すると近似の精度は，$\frac{d_{n\lambda}}{d_{(n+m)\lambda}} = \frac{2n\lambda+1}{2(n+m)\lambda+1} = 1 - \frac{m}{n} \frac{1}{1+\frac{1}{2(n+m)\lambda}}$ となる．ただし，$\mathfrak{g} = \mathfrak{su}(1,1)$ の場合は $2n\lambda < -1$ とする．特に，1 モードのスクイズド状態の場合，$\lambda_1 = -\frac{1}{4}$ であるので，$n > 2, m > 1$ について，$\frac{d_{n\lambda}}{d_{(n+m)\lambda}} = \frac{n-2}{n+m-2}$ となる．2 モードのスクイズド状態の場合，$\lambda = -\frac{1}{2}$ であるので，$m, n > 1$ について，$\frac{d_{n\lambda}}{d_{(n+m)\lambda}} = \frac{n-1}{n+m-1}$ となる．

例 4.5.6 ($\mathfrak{h}_3 \rtimes \mathfrak{u}(1)$ [14]) $\mathfrak{g} = \mathfrak{h}_3 \rtimes \mathfrak{u}(1)$ の場合で $\boldsymbol{\lambda} = (\lambda_Z, \lambda_F)$ のときを考えよう．そして，精度は $\frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}} = \frac{n\lambda_Z}{(n+m)\lambda_Z} = \frac{n}{n+m} = 1 - \frac{m}{n+m}$ となる．

例 4.5.7 ($\mathfrak{su}(r)$[115]) $\mathfrak{g} = \mathfrak{su}(r)$ の場合で $\boldsymbol{\lambda} = [1, 0, \ldots, 0]$ のときを考えよう．精度は $\frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}} = \frac{(n+r-1)!(n+m)!}{(n+m+r-1)!n!}$ となる．

例 4.5.8 $\mathfrak{g} = \mathfrak{h}(2r, \mathbb{R}) \rtimes \mathfrak{u}(r)$ の場合（r モードの Bose 粒子系の場合）で $\boldsymbol{\lambda} = (\lambda_Z, \lambda_F \boldsymbol{v})$ のときを考えよう．そして，精度は $\frac{d_{n\boldsymbol{\lambda}}}{d_{(n+m)\boldsymbol{\lambda}}} = \frac{n^r \lambda_Z^r}{(n+m)^r \lambda_Z^r} = (\frac{n}{n+m})^r$ となる．

1 モードや 2 モードのスクイズド状態の場合や r モードの Bose 粒子系の場合は n, m を整数に限らず，実数としても上記の公式は成り立つ．すなわち，実数個の状態の複製を形式的に考えることができる．

第 5 章

量子誤り訂正とその応用

5.1　古典系での代数的構造に基づいた誤り訂正符号

5.1.1　問題の定式化

群 G の要素を用いて古典的な通信を行うとする．特に，通信途中にノイズがあるとき，入力信号 $g \in G$ に応じて，出力系での $g' \in G$ が決まることになる．以下では，古典系の一般のノイズのある通信路は扱わず，G 上の確率分布 P^G が与えられ，確率 $\mathrm{P}^G(n)$ で入力信号 $g \in G$ が ng に変化して受信するとする．すなわち，確率 $\mathrm{P}^G(n)$ でノイズ $n \in G$ が働くとする．このような設定では，G の部分群 C の要素だけに限って通信することでノイズに対応することができる．この場合，受信信号 g' が C に含まれないとき，ノイズを受けて変化したと考えることができる．剰余類 G/C の要素 x に対して要素の中で最も起こり得るノイズを代表元 g_x として選ぶ．受信信号 $g' \in G$ が剰余類 G/C の要素 x に含まれていたとき，g' を $g_x^{-1}g$ に変換する．すると，確率 $\sum_{x \in G/C} p(g_x)$ で正しく復元できる．1 からこの値を引いた値は誤り確率とよばれる．以下，部分群 C を古典的**符号空間**，代表元 $\{g_x\}_{x \in G/C}$ を古典的**復号化**とよぶ．そして，$M = |C|$ のとき，メッセージ空間 $\{1, \ldots, M\}$ から $C \subset G$ への写像を古典的**符号化**という．特に，各 $x \in G/C$ に対する代表元の選択 $\mathrm{argmax}_{g \in x} \mathrm{P}^G(g)$ を確率分布 P^G の下での古典的符号空間 C の**最尤復号**という．個々の要素 $g \in C$ が等確率で送信されるとすると，最尤復号は

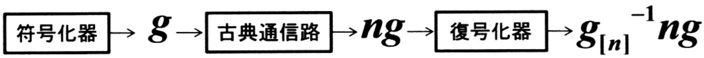


図 5.1　古典通信路での誤り訂正

誤り確率の最小値を実現する．この誤り確率を $\delta[C]$ と記す．

なお，Shannon[104] による定義では，符号空間は G の任意の部分集合を選ぶことが許されている．しかし，符号空間に何らかの代数的な構造を入れない場合，復号化の計算量が極めて大きくなるので，本章では，そのような一般の符号空間は扱わない．本章では部分群として符号空間が与えられる場合を扱う．以下に，$\delta[C]$ の上限を与える．

補題 5.1.1（Gallager[22]）　古典的符号空間 C に対して，最尤復号を用いたときの誤り確率 $\delta[C]$ は任意の $s,t>0$ を用いて，以下のように評価できる．

$$\delta[C] \le \sum_{g\in G} \mathrm{P}^G(g)^{1-st}\left(\sum_{g'\in C\setminus\{e\}} \mathrm{P}^G(gg')^t\right)^s . \tag{5.1}$$

証明.　符号空間 C を用いたときに最尤復号を用いたときの誤り確率は $\delta[C]=\sum_{g\in G}\mathrm{P}^G(g)\Delta_{ML}(g)$ で与えられる．$\Delta_{ML}(g)$ は以下で与えたインジケータ関数である．

$$\Delta_{ML}(g) := \begin{cases} 0 & \text{if } \mathrm{P}^G(g) > \mathrm{P}^G(gg'), \quad \forall g' \in C\setminus\{e\} \\ 1 & \text{otherwise.} \end{cases}$$

ここで，

$$\Delta_{g'}(g) := \begin{cases} 0 & \text{if } \mathrm{P}^G(g) > \mathrm{P}^G(gg'), \\ 1 & \text{otherwise} \end{cases}$$

を用いると，インジケータ関数 $\Delta_{ML}(g)$ は以下のように評価できる．

$$\Delta_{ML}(g) \le \sum_{g'\in C\setminus\{e\}} \Delta_{g'}(g). \tag{5.2}$$

ここで，$s>0$ に対して，(5.2) の両辺を s 乗することによって $\Delta_{ML}(g) \le \left(\sum_{g'\in C\setminus\{e\}}\Delta_{g'}(g)\right)^s$ を得る．さらに，

$$\Delta_{g'}(g) \leq \frac{\mathrm{P}^G(gg')}{\mathrm{P}^G(g)} \tag{5.3}$$

を得る．同じく，$t > 0$ に対して，(5.3) の両辺を t 乗することで $\Delta_{g'}(g) \leq \frac{\mathrm{P}^G(gg')^t}{\mathrm{P}^G(g)^t}$ を得る．これらを要約すると，

$$\Delta_{ML}(g) \leq \left(\sum_{g' \in C \setminus \{e\}} \frac{\mathrm{P}^G(gg')^t}{\mathrm{P}^G(g)^t} \right)^s \tag{5.4}$$

を得る．誤り確率は以下のように評価できる．

$$\begin{aligned} \delta[C] &\leq \sum_{g \in G} \mathrm{P}^G(g) \left(\sum_{g' \in C \setminus \{e\}} \frac{\mathrm{P}^G(gg')^t}{\mathrm{P}^G(g)^t} \right)^s \\ &= \sum_{g \in G} \mathrm{P}^G(g)^{1-st} \left(\sum_{g' \in C \setminus \{e\}} \mathrm{P}^G(gg')^t \right)^s . \end{aligned} \tag{5.5}$$

□

5.1.2　アンサンブルの下での評価

上記の補題から誤りを記述する確率分布 P^G が与えられたとき，符号空間 C の性能はその最尤復号を行ったときの誤り確率で評価できる．しかし，その誤り確率を評価することは一般には容易でない．そのため，符号化のアンサンブルを考え，それぞれに最尤復号を行ったときの誤り確率の平均値を評価することが多い．このような平均値に注目することは，一見すると，問題を複雑にしているように見えるが，確率論的手法が使えるようになり，タイトな評価が可能となる．

以下では G の部分群である符号化をある確率変数 X に応じて選択するとする．すなわち，確率変数 X に基づいて決まる符号空間を C_X と記す．符号空間のアンサンブル C_X が以下を満たすとき，ϵ-ユニバーサル 2 という [13, 109, 111]．

$$\mathrm{P}_X\{C_X \mid g \in C_X\} \leq \epsilon, \quad \forall g \neq e \in G. \tag{5.6}$$

ただし，確率変数 X が従う分布を P_X とした．

そして以下の定理を得る [22, 111].

定理 5.1.2　符号空間のアンサンブル C_X が ϵ-ユニバーサル2であるとき，以下の不等式が成り立つ．

$$\mathrm{E}_X \delta[C_X] \le \min_{0 \le s \le 1} \epsilon^s e^{\phi(s:\mathrm{P}^G)}. \tag{5.7}$$

ただし，$\phi(s:\mathrm{P}^G) := \log\left(\sum_{g \in G} (\mathrm{P}^G(g))^{\frac{1}{1+s}}\right)^{1+s}$ と定義した．

証明.　$0 \le s \le 1$ とし，(5.1) に $t = \frac{1}{1+s}$ を代入すると，

$$\delta[C_X] \le \sum_{g \in G} (\mathrm{P}^G(g))^{\frac{1}{1+s}} \left(\sum_{g' \in C_X \setminus \{e\}} (\mathrm{P}^G(gg'))^{\frac{1}{1+s}} \right)^s$$

を得る．ここで，X について平均をとり，関数 $x \mapsto x^s$ の凸性を用いると，

$$\begin{aligned}
\mathrm{E}_X \delta[C_X] &\le \mathrm{E}_X \sum_{g \in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\sum_{g' \in C_X \setminus \{e\}} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s \\
&\le \sum_{g \in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\mathrm{E}_X \sum_{g' \in C_X \setminus \{e\}} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s \\
&\le \sum_{g \in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\epsilon \sum_{g' \in G} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s
\end{aligned} \tag{5.8}$$

を得る．$\left(\epsilon \sum_{g' \in G} \mathrm{P}^G(gg')^{\frac{1}{1+s}}\right)^s$ は G の要素 g に依存しないので，上記の値は $\left(\epsilon \sum_{g' \in G} \mathrm{P}^G(g')^{\frac{1}{1+s}}\right)^s = \epsilon^s \left(\sum_{g' \in G} \mathrm{P}^G(g')^{\frac{1}{1+s}}\right)^s$ に等しい．したがって，(5.8) の右辺は以下の値に等しい．

$$\begin{aligned}
\sum_{g \in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \epsilon^s \left(\sum_{g' \in G} \mathrm{P}^G(g')^{\frac{1}{1+s}} \right)^s &= \epsilon^s \left(\sum_{g \in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \right)^{1+s} \\
&= \epsilon^s e^{\phi(s:\mathrm{P}^G)}.
\end{aligned} \tag{5.9}$$

□

2つの群 G_1, G_2 の直積群 $G_1 \times G_2$ に適切な ϵ-ユニバーサル2となる符号空間のアンサンブルが見つからないことがある．このような場合，個々の群 G_1, G_2 に ϵ-ユニバーサル2となる符号空間のアンサンブル C_{1,X_1}, C_{2,X_2} が存在すると，これらのアンサンブルから直積群 $G_1 \times G_2$ の符号空間のアンサンブル $C_{1,X_1} \times C_{2,X_2}$ が構成できる．この符号空間のアンサンブルについて以下の定理が成り立つ．

定理 5.1.3 C_{1,X_1} (C_{2,X_2}) を群 G_1 (G_2) の $\epsilon_1(\epsilon_2)$-ユニバーサル2となる符号空間のアンサンブルとする．このとき，直積群 $G_1 \times G_2$ の符号空間のアンサンブル $C_{1,X_1} \times C_{2,X_2}$ は以下を満たす．

$$\begin{aligned} &\mathrm{E}_{X_1,X_2}\delta[C_{1,X_1} \times C_{2,X_2}] \\ &\le \min_{0\le s\le 1} \epsilon_1^s e^{\phi(s:\mathrm{P}^{G_1})} + \min_{0\le s\le 1} \epsilon_2^s e^{\phi(s:\mathrm{P}^{G_2|G_1})}. \end{aligned} \tag{5.10}$$

ただし，$\phi(s:\mathrm{P}^{G_2|G_1}) := \log\left(\sum_{g_1\in G_1}\mathrm{P}^{G_1}(g_1)\left(\sum_{g\in G}(\mathrm{P}^G(g))^{\frac{1}{1+s}}\right)^{1+s}\right)$ と定義した．

証明. 符号空間 $C_{1,X_1} \times C_{2,X_2}$ に対して以下の2段階の復号化法を考える．最尤復号での誤り確率は最小であるので，特定の復号化法で，上記の不等式を示せば十分である．1段階目では，G_1 についての周辺分布 P^{G_1} に基づく最尤復号を行い，ノイズの推測値 $\hat{n}_1$ を得る．そして2段階目では，1段階目でのノイズの推測値 $\hat{n}_1$ に基づき，G_2 の条件付き分布 $\mathrm{P}^{G_2|\hat{n}_1}$ の下での，最尤復号を行い，推測値 $\hat{n}_{2:\hat{n}_1}$ を得る．最後に得られた符号に対して，受信した元 (g_1, g_2) に対して，推測したノイズ $(\hat{n}_1, \hat{n}_{2:\hat{n}_1})$ の逆元を作用し，伝送メッセージを $(\hat{n}_1^{-1}g_1, \hat{n}_{2:\hat{n}_1}^{-1}g_2)$ であると推測する．

したがって，この復号化の下での誤り確率は，$\mathrm{P}\{\hat{n}_1 \neq n_1\} + \mathrm{P}\{\hat{n}_1 = n_1, \hat{n}_{2:\hat{n}_1} \neq n_2\}$ となる．前者の符号空間のアンサンブルについての平均値は定理5.1.2より，$\epsilon_1^s e^{\phi(s:\mathrm{P}^{G_1})}$ で上から押さえることができる．一方，後者については，$\hat{n}_1 = n_1$ が条件となっているので，$\hat{n}_{2:\hat{n}_1}$ を G_2 の条件付き分布 $\mathrm{P}^{G_2|n_1}$ に基づく，最尤復号による推測値 $\hat{n}_{2:n_1}$ に置き換えることができる．よって

$$\mathrm{P}\{\hat{n}_1 = n_1, \hat{n}_{2:\hat{n}_1} \neq n_2\} = \mathrm{P}\{\hat{n}_1 = n_1, \hat{n}_{2:n_1} \neq n_2\} \le \mathrm{P}\{\hat{n}_{2:n_1} \neq n_2\} \tag{5.11}$$

を得る．右辺の値の符号空間のアンサンブルについての平均値は定理 5.1.2 より，

$$\begin{aligned}\mathrm{E}_{X_2}\mathrm{P}\{\hat{n}_{2:n_1} \neq n_2\} &= \mathrm{E}_{X_2}\mathrm{E}_{n_1:\mathrm{P}^{G_1}}\mathrm{P}\{\hat{n}_{2:n_1} \neq n_2\} \\ &= \mathrm{E}_{n_1:\mathrm{P}^{G_1}}\mathrm{E}_{X_2}\mathrm{P}\{\hat{n}_{2:n_1} \neq n_2\} \le \mathrm{E}_{n_1:\mathrm{P}^{G_1}} \min_{0\le s\le 1} \epsilon_2^s e^{\phi(s:\mathrm{P}^{G_2|n_1})}\end{aligned}$$

を得る．よって (5.10) を得る．□

上記の定理 5.1.3 は G の部分群 N が与えられ，N の要素だけ，他の要素と位数が異なる場合などは，G に適切な ϵ-ユニバーサル 2 となる符号空間のアンサンブルが存在しないことが多い．この問題を解決するために，G の符号空間のアンサンブル C_X に対して (ϵ_1, ϵ_2)-二重ユニバーサル 2 の概念を導入する．G の符号空間のアンサンブル C_X が以下の条件を満たすとき，$N \subset G$ に対して (ϵ_1, ϵ_2)-**二重ユニバーサル 2** とよぶことにする．

$$\mathrm{P}_X\{C_X \mid g \in C_X\} \le \epsilon_1, \quad \forall g \in N \setminus \{e\}$$

$$\mathrm{P}_X\{C_X \mid g \in C_X\} \le \epsilon_2, \quad \forall g \in G \setminus N.$$

以下の定理が成り立つ．

定理 5.1.4　C_X を $N \subset G$ に対して (ϵ_1, ϵ_2)-二重ユニバーサル 2 な符号空間のアンサンブルは以下を満たす．

$$\mathrm{E}_X \delta[C_X] \le \min_{0\le s\le 1} \epsilon_2^s e^{\phi(s:\mathrm{P}^G)} + \min_{0\le s\le 1} \epsilon_1^s e^{\phi(s:\mathrm{P}^{N|G/N})}. \tag{5.12}$$

ここで，$\mathrm{P}^G([g]), \mathrm{P}^{[g]}$，および，$\phi(s:\mathrm{P}^{N|G/N})$ は以下で定義した．

$$\mathrm{P}^G([g]) := \sum_{g' \in \mathrm{P}^G([g])} \mathrm{P}^G(g')$$

$$\mathrm{P}^{[g]}(g') := \frac{\mathrm{P}^G(g')}{\mathrm{P}^G([g])}, \quad \forall g' \in [g]$$

$$\phi(s:\mathrm{P}^{N|G/N}) := \log\left(\sum_{[g]\in G/N} \mathrm{P}^G([g]) \left(\sum_{g'\in N} (\mathrm{P}^{[g]}(gg'))^{\frac{1}{1+s}}\right)^{1+s}\right). \tag{5.13}$$

証明. 定理 5.1.2 での (5.8) が以下のように変形できる.

$$
\begin{aligned}
&\mathrm{E}_X \delta[C_X] \\
&\le \sum_{g\in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\epsilon_1 \sum_{g'\in N} \mathrm{P}^G(gg')^{\frac{1}{1+s}} + \epsilon_2 \sum_{g'\in G} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s \\
&\le \sum_{g\in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\epsilon_1 \sum_{g'\in N} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s \\
&\quad + \sum_{g\in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\epsilon_2 \sum_{g'\in G} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s .
\end{aligned}
$$

ここで, $x, y \ge 0$ について $(x+y)^s \le x^s + y^s$ を用いた. 第 2 項は定理 5.1.2 とまったく同じように評価できる. 一方, 第 1 項は

$$
\begin{aligned}
&\sum_{g\in G} \mathrm{P}^G(g)^{\frac{1}{1+s}} \left(\epsilon_1 \sum_{g'\in N} \mathrm{P}^G(gg')^{\frac{1}{1+s}} \right)^s \\
&= \sum_{g\in G/N} \mathrm{P}^G([g]) \sum_{n\in N} \mathrm{P}^{[g]}(gn)^{\frac{1}{1+s}} \left(\epsilon_1 \sum_{g'\in N} \mathrm{P}^{[g]}(gng')^{\frac{1}{1+s}} \right)^s \\
&= \sum_{g\in G/N} \mathrm{P}^G([g]) \epsilon_1^s \left(\sum_{n\in N} \mathrm{P}^{[g]}(gn)^{\frac{1}{1+s}} \right)^{1+s}
\end{aligned}
$$

となり, (5.12) を得る. □

5.1.3 アンサンブルの構成

しかし, 一般の群 G に対して, ϵ-ユニバーサル 2 となる位数が大きい符号空間のアンサンブルを構成することは困難である. 実用的に考えられる群として, 有限体 $\mathbb{F}_q$ 上のベクトル空間 $\mathbb{F}_q^r$ が挙げられる. このとき, $\mathbb{F}_q$ 上の部分ベクトル空間として符号空間 C を構成することが多い. 部分ベクトル空間 C の次元が k であるとき, C は k 個の基底ベクトルを与えることで決まる. k 個の基底ベクトルとなる列ベクトルを横に並べた行列 A を符号空間 C の生成行

列という．したがって，$\mathbb{F}_q^k$ をメッセージ空間と同一視すると，行列 A が符号化を与えることになる．そして，以下の補題が成り立つ [52].

補題 5.1.5　$\mathbb{F}_q$ に一様に値を持つ $r-1$ 個の独立な確率変数 $X=(X_1,\ldots,X_{r-1})$ を与える．$\mathbb{F}_q$ に値を持つ $r-k\times k$ Toeplitz 行列 A_X を以下で定義する．$(A_X)_{l,j}:=X_{r-k-l+j}$ 生成行列を $\begin{pmatrix} I \\ A_X \end{pmatrix}$ とする符号空間を C_X とする．符号化のアンサンブル C_X は q^{k-r}-ユニバーサル 2 となる．

証明.　$\boldsymbol{s}\neq 0\in\mathbb{F}_q^r$ の最初の k 成分が全て 0 の場合は，$\boldsymbol{s}$ が C_X に含まれる確率は 0 である．一方，1 つでも 0 でない成分が $\boldsymbol{s}$ の最初の k 成分に含まれて居ないとする．その中で，最も順番が後ろの成分が第 t 成分であるとする．

$\boldsymbol{s}$ が上記の符号空間に含まれるための必要十分条件は

$$s_{k+l}=X_{r-k-l+t}s_t+\sum_{j=1}^{t-1}X_{r-k-l+j}s_j,\quad l=1,\ldots,r-k \tag{5.14}$$

となる．$l=r-k$ のときの条件 (5.14) に注目する．X_t は $X_{t-1},\ldots,X_1$ と独立であり，X_ts_t は $\mathbb{F}_q$ の全ての要素を確率 $1/q$ でとるので，この条件は確率 $1/q$ で成り立つ．$l=u+1,\ldots,r-k$ のときの条件 (5.14) が成り立つときに，$l=u$ のときの条件 (5.14) が成り立つ確率に注目する．$X_{r-k-u+t}$ は $X_{r-k-u+t-1},\ldots,X_1$ と独立であり，$X_{r-k-u+t}s_t$ は $\mathbb{F}_q$ の全ての要素を確率 $1/q$ でとるので，この条件は確率 $1/q$ で成り立つ．よって，全ての l について条件 (5.14) が成り立つ確率は $1/q^{r-k}$ となる．　□

5.1.4　漸近理論

上記では，群 G の要素を伝送する通信を考え，ノイズが G 上の確率分布 P^G で与えられる場合を扱った．以下では，群 G の r 回の直積群 $G^r:=\overbrace{G\times\cdots\times G}^{r}$ の要素を伝送する通信を考え，ノイズを表す確率分布が P^G の r 次の独立同一分布 $(\mathrm{P}^G)^r$ である場合を扱う．このとき，

$$\phi(s:(\mathrm{P}^G)^r)=r\phi(s:\mathrm{P}^G) \tag{5.15}$$

となる．特に r が無限大の極限を扱う理論は漸近理論とよばれる．このような場合，各 r について，群 G^r の部分群である符号空間 C_r を考え，その系列 $\{C_r\}$ に注目する．そして，最尤復号の下での誤り確率の極限値 $\lim_{r\to\infty}\delta[C_r]$ とその伝送レート $\lim_{r\to\infty}\frac{1}{r}\log|C_r|$ に注目する．漸近理論で重要な役割を果たすのが，エントロピーである．一般に群 G 上の確率分布 P^G のエントロピー $H(\mathrm{P}^G)$ は $H(\boldsymbol{p})$ と同じように，

$$H(\mathrm{P}^G) := -\sum_{g\in G}\mathrm{P}^G(g)\log\mathrm{P}^G(g) \tag{5.16}$$

で与えられる．また，直積群 $G_1\times G_2$ 上の確率分布 P に対して，条件付きエントロピー $H(\mathrm{P}^{G_2|G_1})$ は以下で定義される．

$$H(\mathrm{P}^{G_2|G_1}) := -\sum_{g_1\in G_1}\mathrm{P}^{G_1}(g_1)\sum_{g_2\in G_2}\mathrm{P}^{G_2|g_1}(g_2)\log\mathrm{P}^{G_2|g_1}(g_2). \tag{5.17}$$

条件付きエントロピーは以下を満たす．

$$H(\mathrm{P}^{G_1\times G_2}) = H(\mathrm{P}^{G_2|G_1}) + H(\mathrm{P}^{G_1}). \tag{5.18}$$

G が部分群 G_1 を持つとき，群 G 上の確率分布 P^G の部分群 G_1 についての条件付きエントロピー $H(\mathrm{P}^{G_1|G/G_1})$ は以下で定義される．

$$H(\mathrm{P}^{G_1|G/G_1}) := -\sum_{[g]\in G/G_1}\mathrm{P}^G([g])\sum_{g_1\in G_1}\mathrm{P}^{[g]}(gg_1)\log\mathrm{P}^{[g]}(gg_1). \tag{5.19}$$

そして，以下を得る．

$$H(\mathrm{P}^G) = \lim_{s\to 0}\frac{\phi(s:\mathrm{P}^G)}{s}, \tag{5.20}$$

$$H(\mathrm{P}^{G_1|G/G_1}) = \lim_{s\to 0}\frac{\phi(s:\mathrm{P}^{G_1|G/G_1})}{s}. \tag{5.21}$$

本章では，符号空間は G の部分群として選ぶことになっているが，部分集合として選んだ場合について以下の Shannon による通信路符号化定理が知られている．

定理 5.1.6 (Shannon [104]) 符号空間として G^r 一般の部分集合まで許した場合，誤り確率が 0 に収束する符号の系列の伝送レート最大値は $\log|G| - H(\mathrm{P}^G)$ となる．

次に，

$$R > \frac{H(\mathrm{P}^{\mathbb{F}_q})}{\log q} \tag{5.22}$$

となる R を選び，r に対して k を $k = \lfloor (1-R)r \rfloor$ となるように選ぶ．そして，補題 5.1.5 で与えられた q^{k-r}-ユニバーサル 2 となる符号化のアンサンブルに定理 5.1.2 を適用する．(5.7) の左辺は符号化のアンサンブルについての誤り確率の平均値であるので，最尤復号での誤り確率が (5.7) の右辺以下の符号化が存在する．以下，ここで与えられた符号化の系列について扱う．この符号化の系列の伝送レートは $\log q - R\log q$ となり，(5.15) より，(5.7) の右辺は，$e^{-r\max_{0\le s\le 1}(sR\log q - \phi(s:\mathrm{P}^{\mathbb{F}_q}))}$ となる．(5.20) が成り立つから，条件 (5.22) より，十分小さい $s > 0$ を選ぶと，$R\log q > \frac{\phi(s:\mathrm{P}^{\mathbb{F}_q})}{s}$ となる．したがって，$\max_{0\le s\le 1}(sR\log q - \phi(s:\mathrm{P}^{\mathbb{F}_q})) > 0$ となり，(5.7) の右辺は r について指数的に 0 に収束する．したがって，誤り確率が 0 に収束し，伝送レートが $\log q - H(\mathrm{P}^{\mathbb{F}_q})$ に十分近い符号の列が存在する．そして，定理 5.1.6 より，この方法で与えたものが，漸近的に最適な伝送レートを達成する．

5.1.5　秘匿性を伴った誤り訂正

一方，部分的に盗聴を受けていたとすると，盗聴者に対して送りたかった情報が何であるかわからないようにする工夫が必要である．そのため，実際に伝送するメッセージを C の要素とするのではなく，C の正規部分群 N を考え，剰余群 C/N の要素をメッセージとする方法が考えられる [116]．このように，伝送する情報を部分群で割って得られる剰余群 C/N の要素とすることで秘匿性を確保する方法を**秘匿性増強**とよぶ．この場合，上記と同じノイズを表す確率分布 P^G と古典的復号化 $\mathcal{J} := \{g_x\}_{x\in G/C}$ の下で，正しく復号できる確率は $\mathrm{P}^G(\mathcal{J}N) := \sum_{x\in G/C, n\in N}\mathrm{P}^G(g_x n)$ で与えられる．特に，メッセージ $[g] \in C/N$ が誤って $[g'g] \in C/N$ に復号される確率は $\mathrm{P}^G\{\mathcal{J},N\}^{C/N}([g']) := \mathrm{P}^G(\mathcal{J}g'N)$ で与えられる．

この場合，部分群の対 $N \subset C$ を**符号化対**とよぶ．特に，各 $x \in G/C$ に対する代表元の選択 $\mathrm{argmax}_{g\in x}\sum_{n\in N}\mathrm{P}^G(gn)$ を確率分布 P^G の下での古典的符号化対 $N \subset C$ の**最尤復号**という．この場合，正しく復元できる確率が最大とする．このときの誤り確率を $\delta_{\mathrm{P}^G}[C/N]$ と記す．分布 P^G を明記しなくて

も混乱の恐れがない場合は $\delta[C/N]$ と記す.

問題によって, あらかじめ, 正規部分群 N が決まっており, N を含む符号空間 C をある確率変数 X に応じてランダムに選ぶことが可能である場合がある. このような場合, $N \subset G$ に対する $(1,\epsilon)$-二重ユニバーサル2な符号空間のアンサンブル C_X を用いることになる. このようなアンサンブルの構成は G/N に対する符号空間のアンサンブルから以下のように構成できる.

補題 5.1.7 N を正規部分群とし, G から G/N への準同型を π_N と記す. このとき, G/N の ϵ-ユニバーサル2となる符号空間のアンサンブル C_X に対して, $\pi_N^{-1}(C_X)$ は $N \subset G$ に対する $(1,\epsilon)$-二重ユニバーサル2な符号空間のアンサンブルとなる.

この補題により, 5.1.3項で構成した符号化のアンサンブルを下に, 本項で必要となる符号化のアンサンブルが構成できる.

初めに補題5.1.1の一般化として以下の補題を得る. 証明は $G\setminus\{e\}$ を $G\setminus N$ と書き換えることで得られる.

補題 5.1.8 部分群 N を含む古典的符号空間 C に対して, 最尤復号を用いたときの誤り確率 $\delta[C]$ は任意の $s,t>0$ を用いて, 以下のように評価できる.

$$\delta[C/N] \le \sum_{g\in G} \mathrm{P}^G(g)^{1-st}\left(\sum_{g'\in C\setminus N} \mathrm{P}^G(gg')^t\right)^s .$$

そして, 定理5.1.2の一般化として以下を得る. 以下の定理5.1.9の証明は定理5.1.2の証明において, $G\setminus\{e\}$ を $G\setminus N$ と書き換えることで得られる.

定理 5.1.9 符号空間のアンサンブル C_X が $N \subset G$ に対する $(1,\epsilon)$-二重ユニバーサル2であるとき, 不等式 $\mathrm{E}_X\delta[C_X] \le \min_{0\le s\le 1} \epsilon^s e^{\phi(s:\mathrm{P}^G)}$ が成り立つ.

5.2 量子誤り訂正の一般理論

量子系 $\mathcal{H}$ に通信中にノイズが加わる場合での状態変化は量子系 $\mathcal{H}$ 上のトレースを保存する完全正写像で与えられる. 量子系でのノイズに対抗して量子



図 5.2　量子通信路での誤り訂正

状態を正確に伝送するための方法として，実際に伝送する量子系を $\mathcal{H}$ の部分空間 $\mathcal{H}_0$ に制限する方法が考えられる．この場合，出力系で，$\mathcal{H}_0$ から外れた状態を $\mathcal{H}_0$ に戻すことで，特定のタイプのノイズを打ち消すことが可能となる．このように，部分空間 $\mathcal{H}_0$ を**符号化**とよび，$\mathcal{H}$ から $\mathcal{H}_0$ へのトレースを保存する完全正写像を**復号化**とよび，これらの組を**量子誤り訂正**とよぶ．例えば，量子系 $\mathcal{H}$ が量子系 $\bigoplus_{i=0}^k \mathcal{H}_i$ で与えられており，ノイズを与えるトレースを保存する完全正写像の Kraus 表現が

$$\Lambda(\rho) := \sum_{i=0}^{k} \sqrt{p_i} U_i \rho \sqrt{p_i} U_i^\dagger \tag{5.23}$$

で与えられるとする．ここで，U_i は $\mathcal{H}_0$ を $\mathcal{H}_i$ に移すユニタリ行列とし，p_i を確率とする．このとき，復号化を $D(\rho) := \sum_{i=0}^k (U_i P_i)^\dagger \rho P_i U_i$ で与える．ただし，P_i は $\mathcal{H}_i$ への射影である．すると，ρ が $\mathcal{H}_0$ 上の状態（すなわち，ρ のサポートが $\mathcal{H}_0$ に含まれる）であるとき，$D \circ \Lambda(\rho) = \rho$ となる．このように，ノイズの形が (5.23) のように理想的な形で与えられているとき，符号化 $\mathcal{H}_0$ と復号化 D の組み合わせで完全に量子的なノイズが除去できる．

しかし，一般の量子系のノイズは (5.23) のように理想的な形では与えられない．符号化 $\mathcal{H}_0$ を持つ量子誤り訂正の性能は量子通信路 $D \circ \Lambda_{\mathcal{H}_0}$ のエンタングルメント忠実度 $F_e^2(D \circ \Lambda_{\mathcal{H}_0})$ によって評価される．Λ の Kraus 表現が $\Lambda(\rho) := \sum_j F_i \rho F_i^\dagger$ で与えられるとき，$D\circ\Lambda_{\mathcal{H}_0}$ の Kraus 表現は $(D\circ\Lambda_{\mathcal{H}_0})(\rho) = \sum_{j,i} (U_i P_i F_j^\dagger)^\dagger \rho F_j^\dagger P_i U_i$ で与えられる．したがって，(2.41) を用いると，量子通信路 $D \circ \Lambda_{\mathcal{H}_0}$ のエンタングルメント忠実度は $F_e^2(D \circ \Lambda_{\mathcal{H}_0}) = \sum_{j,i} |\frac{\mathrm{Tr}\, F_j^\dagger P_i U_i}{\mathrm{Tr}\, P_0}|^2$ で与えられる．

5.3　離散 Heisenberg 表現を用いた符号

5.3.1　離散 Heisenberg 表現の復習

次に，量子誤り訂正符号の中で代表的なクラスとして，Stabilizer 符号を扱

うが，そのための準備として簡単に離散 Heisenberg 表現について復習しよう．より詳しい内容については，[37, 第 7 章] を参照のこと．初めに，環 $\mathbb{Z}_d$ 上の離散 Heisenberg 表現について復習しよう．

しかし，射影的ユニタリ表現については，既約な d 次元のものが構成できる．初めに計算基底 $\{|0\rangle, \ldots, |d-1\rangle\}$ を正規直交基底系とする空間 $\mathcal{H}$ 上の行列 $\mathsf{X}_{\mathbb{Z}}, \mathsf{Z}_{\mathbb{Z}}$ を以下のように定義する．

$$\mathsf{X}_{\mathbb{Z}}|x\rangle = |x+1\rangle, \quad \mathsf{Z}_{\mathbb{Z}}|x\rangle = \omega_{\mathbb{Z}}^{x}|x\rangle. \tag{5.24}$$

ここで，$\omega_{\mathbb{Z}} := e^{i2\pi/d}$ とした．この定義は以下と同値である．

$$\mathsf{X}_{\mathbb{Z}} = \sum_{x} |x+1\rangle\langle x|, \quad \mathsf{Z}_{\mathbb{Z}} = \sum_{x} \omega_{\mathbb{Z}}^{x}|x\rangle\langle x|. \tag{5.25}$$

そして，W を以下で定義する．

$$\tilde{\mathsf{W}}_{\mathbb{Z}}(s,t) := \mathsf{X}^{s}\mathsf{Z}^{t} = \sum_{s} \omega_{\mathbb{Z}}^{xt}|x+s\rangle\langle x|, \quad \forall (s,t) \in \mathbb{Z}_d^2. \tag{5.26}$$

すると，$\omega_{\mathbb{Z}}\mathsf{XZ} = \mathsf{ZX}$ が成立するので，

$$\tilde{\mathsf{W}}_{\mathbb{Z}}(s,t)\tilde{\mathsf{W}}_{\mathbb{Z}}(s',t') = \omega_{\mathbb{Z}}^{s't}\tilde{\mathsf{W}}_{\mathbb{Z}}(s+s',t+t') \tag{5.27}$$

が成り立ち，$\tilde{\mathsf{W}}_{\mathbb{Z}}$ は $\mathbb{Z}_d^2$ の射影的ユニタリ表現となる．

ここで，d が奇数の場合，$\tau_{\mathbb{Z}} := \omega_{\mathbb{Z}}^{(d+1)/2}$ とし，d が偶数の場合，$\tau_{\mathbb{Z}} := e^{i\pi/d}$ とおいて，射影的ユニタリ表現 $\mathsf{W}_{\mathbb{Z}}(s,t)$ を以下で与える．

$$\mathsf{W}_{\mathbb{Z}}(s,t) := \tau_{\mathbb{Z}}^{st}\tilde{\mathsf{W}}_{\mathbb{Z}}(s,t) = \tau_{\mathbb{Z}}^{st}\sum_{s} \omega_{\mathbb{Z}}^{xt}|x+s\rangle\langle x|. \tag{5.28}$$

st は 0 から $d-1$ までの整数を与えるとする．すると，

$$\mathsf{W}_{\mathbb{Z}}(s,t)\mathsf{W}_{\mathbb{Z}}(s',t') = \begin{cases} \tau_{\mathbb{Z}}^{s't-t's}\mathsf{W}_{\mathbb{Z}}(s+s',t+t') & d \text{ が奇数のとき} \\ (-1)^{\epsilon}\tau_{\mathbb{Z}}^{s't-t's}\mathsf{W}_{\mathbb{Z}}(s+s',t+t') & d \text{ が偶数のとき} \end{cases} \tag{5.29}$$

が成り立つ．ここで，ϵ は s,t,s',t' によって決まる 0 または 1 の整数である．$\mathsf{W}_{\mathbb{Z}}(s,t)$ を $\mathbb{Z}_d^2$ の**離散 Heisenberg 表現**とよぶ．

ここで，計算基底 $\{|x\rangle\}_{x\in\mathbb{Z}_d}$ に対して，**双対計算基底**

$$|\hat{e}_{\mathbb{Z}}(l)\rangle := \frac{1}{\sqrt{d}}\sum_{k\in\mathbb{Z}_d}\omega_{\mathbb{Z}}^{-kl}|k\rangle, \quad l\in\mathbb{Z}_d \tag{5.30}$$

を定義すると，双対計算基底は $\mathsf{X}_{\mathbb{Z}}$ の固有ベクトルになる．$\mathsf{Z}_{\mathbb{Z}}$ は双対計算基底を移す作用となる．

そして，群 $\mathrm{H}(2,\mathbb{Z}_d)$ について $\mathsf{W}_{\mathbb{Z},\mathrm{H}}$ を以下で定義する．

$$\begin{aligned}\mathsf{W}_{\mathbb{Z},\mathrm{H}}(s,t,\omega_d^n) &:= \tau_{\mathbb{Z}}^n\mathsf{W}_{\mathbb{Z}}(s,t) \quad d\text{が奇数のとき}\\ \mathsf{W}_{\mathbb{Z},\mathrm{H}}(s,t,\omega_{2d}^n) &:= \tau_{\mathbb{Z}}^n\mathsf{W}_{\mathbb{Z}}(s,t) \quad d\text{が偶数のとき}.\end{aligned}$$

すると，$\mathsf{W}_{\mathbb{Z},\mathrm{H}}$ はユニタリ表現となる．この事実は，[37] の (7.7) で与えられる因子団に基づく $\mathbb{Z}_d^2$ の中心拡大が [37] の例 2.2.3 で与えた離散 Heisenberg 群 $\mathrm{H}(2,\mathbb{Z}_d)$ と同型であることから確認できる．

次に，有限体 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ のガロワ拡大 $\mathbb{F}_q$ が与えられた場合について考える．初めに計算基底 $\{|x\rangle\}_{x\in\mathbb{F}_q}$ を正規直交基底系とする空間 $\mathcal{H}$ 上の行列 $\mathsf{X}_{\mathbb{F}}, \mathsf{Z}_{\mathbb{F}}$ を以下のように定義する．

$$\mathsf{X}_{\mathbb{F}}(s)|x\rangle = |x+s\rangle, \quad \mathsf{Z}_{\mathbb{F}}(t)|x\rangle = \omega_{\mathbb{F}}^{trtx}|x\rangle. \tag{5.31}$$

ここで，$\omega_{\mathbb{F}} := e^{i2\pi/p}$ とし，$\mathbb{F}_q$ をベクトル空間 $\mathbb{F}_p^m$ と見なしたときに掛け算 $x\mapsto zx$ を行列表示したものを M_z としたとき，$\mathrm{Tr}\, M_z$ を trz と表した．この定義は以下と同値である．

$$\mathsf{X}_{\mathbb{F}}(s) = \sum_{x\in\mathbb{F}_q}|x+s\rangle\langle x|, \quad \mathsf{Z}_{\mathbb{F}}(t) = \sum_{x\in\mathbb{F}_q}\omega_{\mathbb{Z}}^{trtx}|x\rangle\langle x|.$$

そして，$\mathsf{X}_{\mathbb{F}}(s)\mathsf{Z}_{\mathbb{F}}(t)\mathsf{X}_{\mathbb{F}}(-s) = \omega_{\mathbb{F}}^{-trst}\mathsf{Z}_{\mathbb{F}}(t)$ が成り立つので，$\tilde{\mathsf{W}}_{\mathbb{F}}(s,t) := \mathsf{X}_{\mathbb{F}}(s)\mathsf{Z}_{\mathbb{F}}(t) = \sum_{x\in\mathbb{F}_q}\omega_{\mathbb{Z}}^{trtx}|x+s\rangle\langle x|, \quad \forall(s,t)\in\mathbb{F}_q^2$ は $\tilde{\mathsf{W}}_{\mathbb{F}}(s,t)\tilde{\mathsf{W}}_{\mathbb{F}}(s',t') = \omega_{\mathbb{F}}^{trs't}\tilde{\mathsf{W}}_{\mathbb{F}}(s+s',t+t')$ を満たす．よって，$\tilde{\mathsf{W}}_{\mathbb{F}}$ は $\mathbb{F}_q^2$ の射影的ユニタリ表現となる．

ここで，$\mathbb{F}_q$ の標数 p が 2 でないときは，$\tau_{\mathbb{F}} := \omega_{\mathbb{Z}}^{(p+1)/2}$ とし，標数 p が 2 の場合，$\tau_{\mathbb{F}} := i$ とおいて，射影表現 $\mathsf{W}_{\mathbb{F}}(s,t)$ を以下で与える．

$$\mathsf{W}_{\mathbb{F}}(s,t) := \tau_{\mathbb{F}}^{trts}\tilde{\mathsf{W}}_{\mathbb{F}}(s,t) = \tau_{\mathbb{F}}^{trts}\sum_{x\in\mathbb{F}_q}\omega_{\mathbb{F}}^{trtx}|x+s\rangle\langle x|.$$

$trts$ は 0 から $p-1$ までの整数を与えるとする．

すると，

$$\mathsf{W}_{\mathbb{F}}(s,t)\mathsf{W}_{\mathbb{F}}(s',t') = \begin{cases} \tau_{\mathbb{F}}^{tr(s't-t's)}\mathsf{W}_{\mathbb{F}}(s+s',t+t') & p \neq 2 \\ (-1)^{\epsilon}\tau_{\mathbb{F}}^{tr(s't-t's)}\mathsf{W}_{\mathbb{F}}(s+s',t+t') & p = 2 \end{cases} \tag{5.32}$$

が成り立つ．ここで，ϵ は s,t,s',t' によって決まる 0 または 1 である整数である．$\mathbb{F}_q^2$ の射影的ユニタリ表現 $\mathsf{W}_{\mathbb{F}}(s,t)$ を $\mathbb{F}_q^2$ の**離散 Heisenberg 表現**とよぶ．q が素数 p であるときは，$\mathbb{F}_p^2$ と $\mathbb{Z}_p^2$ を同一視することで，$\mathbb{F}_p^2$ の離散 Heisenberg 表現と $\mathbb{Z}_p^2$ の離散 Heisenberg 表現は一致する．しかし，q が素数 p の冪 p^m であるときは，$\mathbb{F}_q^2$ の離散 Heisenberg 表現と $\mathbb{Z}_q^2$ の離散 Heisenberg 表現は一致しない．

ここで，計算基底 $\{|x\rangle\}_{x\in\mathbb{F}_q}$ に対して，**双対計算基底**

$$|\hat{e}_{\mathbb{F}}(l)\rangle := \frac{1}{\sqrt{q}}\sum_{k\in\mathbb{F}_q}\omega_{\mathbb{F}}^{-trkl}|k\rangle, \quad l\in\mathbb{F}_q \tag{5.33}$$

を定義すると，双対計算基底は $\mathsf{X}_{\mathbb{F}}$ の固有ベクトルになる．$\mathsf{Z}_{\mathbb{F}}$ は双対計算基底を移す作用となる．

次に，$\mathbb{Z}_d^2$ または $\mathbb{F}_q^2$ の離散 Heisenberg 表現から群 $\mathbb{Z}_d^{2r}$ またはベクトル空間 $\mathbb{F}_q^{2r}$ の $\mathcal{H}^{\otimes r} = \mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_r$ への射影的ユニタリ表現を以下のように定義する．ここで，$\mathcal{H}_i$ は $\mathcal{H}$ と同型な空間である．空間 $\mathcal{H}^{\otimes r}$ の計算基底は，$\mathbb{Z}_d^r$ または $\mathbb{F}_q^r$ の要素 s を用いて，$|s\rangle$ と表すことができる．以下では $\mathbb{X}=\mathbb{F}_q,\mathbb{Z}_d$ とし，$\mathsf{W}_{\mathbb{X},i}(s,t)$ を i 番目の空間 $\mathcal{H}_i$ への $\mathsf{W}_{\mathbb{X}}(s,t)$ の作用として定義し，以下を定義する．

$$\mathsf{W}_{\mathbb{X}}^r(\vec{s}) := \mathsf{W}_{\mathbb{X},1}(s_1,t_1)\otimes\cdots\otimes\mathsf{W}_{\mathbb{X},r}(s_r,t_r), \forall\vec{s}=(s_1,\ldots s_r,t_1,\ldots,t_r)\in\mathbb{X}^{2r}.$$

したがって，$\boldsymbol{s}=(s_1,\ldots s_r),\boldsymbol{t}=(t_1,\ldots t_r)\in\mathbb{X}^r$ に対して，$(\boldsymbol{s},\boldsymbol{t})_{\mathbb{Z}} := s_1t_1+\cdots+s_rt_r$, $(\boldsymbol{s},\boldsymbol{t})_{\mathbb{F}} := tr(s_1t_1+\cdots+s_rt_r)$ を定義し，$\vec{s}=(\boldsymbol{s},\boldsymbol{t}),\vec{s}'=(\boldsymbol{s}',\boldsymbol{t}')\in\mathbb{X}^{2r}$ に対して，$\langle\vec{s},\vec{s}'\rangle_{\mathbb{X}} := (\boldsymbol{s}',\boldsymbol{t})_{\mathbb{X}} - (\boldsymbol{s},\boldsymbol{t}')_{\mathbb{X}}$ を定義すると，

$$\mathsf{W}_{\mathbb{X}}^r(\vec{s})\mathsf{W}_{\mathbb{X}}^r(\vec{s}') = \begin{cases} \tau_{\mathbb{X}}^{\langle\vec{s},\vec{s}'\rangle_{\mathbb{X}}}\mathsf{W}_{\mathbb{X}}^r(\vec{s}+\vec{s}') & d \text{ または } p \text{ が奇数} \\ (-1)^{\epsilon}\tau_{\mathbb{X}}^{\langle\vec{s},\vec{s}'\rangle_{\mathbb{X}}}\mathsf{W}_{\mathbb{X}}^r(\vec{s}+\vec{s}') & d \text{ または } p \text{ が偶数} \end{cases} \tag{5.34}$$

が成り立つ．ここで，ϵ は s, t, s', t' によって決まる 0 または 1 である整数である．よって，$\mathsf{W}^r_{\mathbb{Z}}, \mathsf{W}^r_{\mathbb{F}}$ は $\mathbb{Z}_d^{2r}$, $\mathbb{F}_q^{2r}$ の射影的ユニタリ表現となる．射影的ユニタリ表現 $\mathsf{W}^r_{\mathbb{Z}}, \mathsf{W}^r_{\mathbb{F}}$ を $\mathbb{Z}_d^{2r}$ または $\mathbb{F}_q^{2r}$ の**離散 Heisenberg 表現**とよぶ．

5.3.2　Stabilizer 符号

上述の準備の下で，$\mathbb{X}$ を $\mathbb{F}_q$ または $\mathbb{Z}_d$ として，離散 Heisenberg 表現の下で誤り訂正符号を構成する [10, 11, 24, 29]．表現空間 $\mathcal{H}$ 上の $\mathbb{X}^{2r}$ の既約な射影的ユニタリ表現 $\mathsf{W}^r_{\mathbb{X}}$ が与えられた場合を考える．このとき，$\mathbb{X}^{2r}$ の自己直交部分群 N （すなわち，$N \subset N^{\perp}$ を満たす部分群）が与えられれば，表現空間の直和分解 $\mathcal{H} = \bigoplus_{\vec{s} \in N^*} \mathcal{H}_x$ が得られる．$\mathsf{W}^r_{\mathbb{X}}(\vec{s})$ は $\mathcal{H}_x$ を $\mathcal{H}_{x+[\vec{s}]}$ に移す．（これら 2 つの事実については [37] の 7.1.4 項を参照）．したがって，$\mathcal{H}_x$ への射影を P_x とすると，

$$\mathsf{W}^r_{\mathbb{X}}(\vec{s}) P_x = P_{x+[\vec{s}]} \mathsf{W}^r_{\mathbb{X}}(\vec{s}) P_x = P_{x+[\vec{s}]} \mathsf{W}^r_{\mathbb{X}}(\vec{s}) \tag{5.35}$$

が成り立つ．

この構造を利用して，量子誤り訂正を構成しよう．初めに符号化を $\mathcal{H}_0$ とする．あらかじめ，$x \in N^* = \mathbb{X}^{2r}/N^{\perp}$ 要素に対して代表元 $\vec{s}_x$ を選んでおく．射影測定 $\{P_x\}_{x \in N^*}$ を行い，測定値 $x \in N^*$ を得る．$x \neq 0$ のとき，エラーの影響で空間 $\mathcal{H}_0$ からはみ出て $\mathcal{H}_x$ に移ったと考えられる．このとき，$x \subset \mathbb{X}^{2r}$ の要素が働いて $\mathcal{H}_0$ から $\mathcal{H}_x$ に移ったと考える．x の代表元 $\vec{s}_x$ が働いたと判断して，$\mathsf{W}^r_{\mathbb{X}}(\vec{s}_x)^\dagger$ を施すことで，誤り $\mathsf{W}^r_{\mathbb{X}}(\vec{s}_x)$ を訂正する．この操作を数学的に記述すると $D(\rho) := \sum_{x \in N^*} \mathsf{W}^r_{\mathbb{X}}(\vec{s}_x)^\dagger P_x \rho P_x \mathsf{W}_{\mathbb{X}}(\vec{s}_x)$ となる．ここで，代表元 $\vec{s}_x$ の選び方として，必ずしも，代表元の集合 $\mathcal{J} := \{\vec{s}_x\}$ が部分群となるように選ぶ必要はない．部分群となるように選ぶと都合がよいことがあるが，実際のノイズに対して有効に誤り訂正が働くには，むしろ，$\{\vec{s}_x\}$ が部分群とならないように選んだ方が有利である．自己直交部分群 N から上記の方法で構成される量子誤り訂正符号を自己直交部分群 N を **Stabilizer** とする **Stabilizer 符号**とよぶ．例えば，Pauli 通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}](\rho) = \sum_{\vec{s} \in \mathbb{X}^{2r}} \mathrm{P}^{\mathbb{X}^{2r}}(\vec{s}) \mathsf{W}^r_{\mathbb{X}}(\vec{s}) \rho \mathsf{W}^r_{\mathbb{X}}(\vec{s})^\dagger$ の場合，確率 $\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s})$ で誤り $\mathsf{W}^r_{\mathbb{X}}(\vec{s})$ が起きると見なせる．以下，$\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]$ を $\Lambda[\mathrm{P}^{\mathbb{X}^{2r}}]$ と略す．

$\vec{s} \in \mathbb{X}^{2r}$ について，$x = [\vec{s}]$ とすると，[37] の (7.24) より，

$$\operatorname{Tr} \mathsf{W}_{\mathbb{X}}^r(\vec{s} - \vec{s}_x)|_{\mathcal{H}_0} = \begin{cases} 0 & \vec{s} - \vec{s}_x \notin N \text{ であるとき} \\ \operatorname{Tr} P_0 & \vec{s} - \vec{s}_x \in N \text{ であるとき} \end{cases}$$

となる．この場合，(2.41) より，量子通信路 $D \circ \Lambda_{\mathcal{H}_0}$ のエンタングルメント忠実度は

$$F_e^2(D \circ \Lambda_{\mathcal{H}_0}) = \sum_{x \in N^*, \vec{s} \in N} \mathrm{P}^{\mathbb{X}^{2r}}(\vec{s}_x + \vec{s}) = \mathrm{P}^{\mathbb{X}^{2r}}(\mathcal{J} + N)$$

となる．$\mathcal{H}_0$ の代わりに $\mathcal{H}_{x'}$ を符号空間とした場合，

$$D_{x'}(\rho) := \sum_{x \in N^*} \mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x-x'})^\dagger P_x \rho P_x \mathsf{W}_{\mathbb{X}}(\vec{s}_{x-x'})$$

とすると，同等の誤り訂正能力がある．このとき，自然に $\mathcal{H}_0$ や一般の $\mathcal{H}_x$ に対して，自然に群 $N^\perp/N$ の表現が定義できる．以下では，この表現を $\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_x}$ と記す．一般に，$[\vec{s}] \in N^\perp/N$ に対して，確率分布　$\mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J}+N\}^{N^\perp/N}([\vec{s}]) := \mathrm{P}^{\mathbb{X}^{2r}}(\mathcal{J} + \vec{s} + N)$ を定義すると，

$$\begin{aligned} &P[D_x \circ \Lambda_{\mathcal{H}_x}]([\vec{s}]) \\ &= \frac{1}{\dim \mathcal{H}_x^2} \langle\langle \mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_x}([\vec{s}])|((D_x \circ \Lambda_{\mathcal{H}_x}) \otimes id)(|I_{\mathcal{H}_x}\rangle\rangle\langle\langle I_{\mathcal{H}_x}|)|\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_x}([\vec{s}])\rangle\rangle \\ &= \mathrm{P}^{\mathbb{X}^{2r}}(\mathcal{J} + \vec{s} + N) = \mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J} + N\}^{N^\perp/N}([\vec{s}]) \end{aligned}$$

となる．したがって，$D \circ \Lambda_{\mathcal{H}_x}$ は Pauli 通信路であるので，$D \circ \Lambda_{\mathcal{H}_x} = \Lambda[\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_x}, \mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J} + N\}^{N^\perp/N}]$ を得る．すなわち，誤り訂正を行って得られる通信路は確率分布　$\mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J} + N\}$ で記述される Pauli 通信路となる．

与えられた符号化空間 $\mathcal{H}_0$ と Pauli 通信路の下で，最もエンタングルメント忠実度を最も大きくする復号化は，各 $x \in N^*$ に対して，代表元 $\operatorname{argmax}_{\vec{s}_x \in x} \sum_{\vec{s} \in N} \mathrm{P}^{\mathbb{X}^{2r}}(\vec{s}_x + \vec{s})$ を選ぶことで得られる．この復号化を確率分布 $\mathrm{P}^{\mathbb{X}^{2r}}$ の下での符号化 N の**最尤復号**とよぶ．また，[37] の補題 7.1.8 より，この符号の符号空間 $\mathcal{H}_0$ の次元は $|\mathbb{X}|^r/|N^*|$ である．このように，Stabilizer 符号の復号化の構成やそのエンタングルメント忠実度の評価は確率分布 $\mathrm{P}^{\mathbb{X}^{2r}}$ に基づく古典的な議論に帰着される．

5.3.3 CSS 符号

本項では，$\mathbb{X}^{2r} = \mathbb{X}^r \times \mathbb{X}^r$ となる構造を利用して，Stabilizer 符号を構成する [12, 107, 30]．以下の議論では，$\mathbb{X}^{2r}$ の第1成分と第2成分を区別するため，それぞれを区別する必要があるときには $\mathbb{X}_1^r, \mathbb{X}_2^r$ と記すことにする．そして，部分群 $C \subset \mathbb{X}^r$ に対して，C の**直交部分群** $C^{\perp} := \{\boldsymbol{s} \in \mathbb{X}^r \mid (\boldsymbol{s}, \boldsymbol{t})_{\mathbb{X}} = 0,\ \forall \boldsymbol{t} \in C\}$ を定義すると，以下の補題が成り立つ．

補題 5.3.1　$C_2^{\perp} \times C_1^{\perp} = (C_1 \times C_2)^{\perp}$ が成り立つ．

証明.　$C_2^{\perp} \times C_1^{\perp} \subset (C_1 \times C_2)^{\perp}$ は容易に確認できる．逆に，$(\boldsymbol{s}, \boldsymbol{t}) \in (C_1 \times C_2)^{\perp}$ は任意の $\boldsymbol{s}' \in C_1, \boldsymbol{t}' \in C_2$ について，$(\boldsymbol{s}', \boldsymbol{t})_{\mathbb{X}} = (\boldsymbol{s}, \boldsymbol{t}')_{\mathbb{X}}$ を満たす．$\boldsymbol{s}' = 0$ のときを考えると，$\boldsymbol{s} \in C_2^{\perp}$ を得る．$\boldsymbol{t}' = 0$ のときを考えると，$\boldsymbol{t} \in C_1^{\perp}$ となり，題意を得る． □

2つの部分群 $C_1, C_2 \subset \mathbb{X}^r$ が**ねじれ条件**: $C_1 \subset C_2^{\perp}$ を満たすとき，$C_2 \subset C_1^{\perp}$ が成り立ち，$N := C_1 \times C_2 \subset \mathbb{X}^{2r}$ は自己直交部分群となる．この自己直交部分群に基づく Stabilizer 符号を Calderbank-Shor-Smolin (**CSS**) **符号**とよぶ．このとき，補題5.3.1より，$(C_1 \times C_2)^*$ は $\mathbb{X}^r/C_2^{\perp} \times \mathbb{X}^r/C_1^{\perp}$ と同型となる．この事実より，CSS 符号の符号空間 $\mathcal{H}_0$ の次元は以下の式で与えられる．

$$\frac{|\mathbb{X}|^r}{|N^*|} = \frac{|\mathbb{X}|^r}{|\mathbb{X}^r/C_2^{\perp}| \cdot |\mathbb{X}^r/C_1^{\perp}|} = \frac{|C_2^{\perp}| \cdot |C_1^{\perp}|}{|\mathbb{X}|^r}. \tag{5.36}$$

そして，$[\boldsymbol{s}] \in C_2^{\perp}/C_1$ に対して一意に定まるベクトル $|[\boldsymbol{s}]\rangle := \sum_{\boldsymbol{s}' \in [\boldsymbol{s}]} \frac{1}{\sqrt{|C_1|}} |\boldsymbol{s}'\rangle$ を定義する．すると，$\mathcal{H}_0$ の正規直交基底は $\{|[\boldsymbol{s}]\rangle\}_{[\boldsymbol{s}] \in C_2^{\perp}/C_1}$ で与えられる．上記のベクトルの一般化として，$([\boldsymbol{x}], [\boldsymbol{y}]) \in \mathbb{X}^r/C_2^{\perp} \times \mathbb{X}^r/C_1^{\perp} = (C_1 \times C_2)^*$ と $[\boldsymbol{s}] \in C_2^{\perp}/C_1$ に対して一意に定まるベクトル

$$|[\boldsymbol{s}], [\boldsymbol{x}], [\boldsymbol{y}]\rangle := \sum_{\boldsymbol{s}' \in [\boldsymbol{s}]} \frac{1}{\sqrt{|C_1|}} \omega_{\mathbb{X}}^{\boldsymbol{s}' \cdot \boldsymbol{y}} |\boldsymbol{s}' + \boldsymbol{x}\rangle$$

を定義する．すると，$\mathcal{H}_{([\boldsymbol{x}],[\boldsymbol{y}])}$ の正規直交基底は $\{|[\boldsymbol{s}], [\boldsymbol{x}], [\boldsymbol{y}]\rangle\}_{[\boldsymbol{s}] \in C_2^{\perp}/C_1}$ で与えられる．

また，補題5.3.1より，$x \in \mathbb{X}^r/C_2^{\perp}$, $y \in \mathbb{X}^r/C_1^{\perp}$ に対して，それぞれの代表元 $\boldsymbol{s} \in x \subset \mathbb{X}^r$, $\boldsymbol{t} \in y \subset \mathbb{X}^r$ を用いて，$(x, y) \in (C_1 \times C_2)^*$ の代表元

$(\boldsymbol{s},\boldsymbol{t}) \in (x,y) \subset \mathbb{X}^{2r}$ が与えられる．このとき，x の代表元 $\boldsymbol{s}$ を y に依存して選ぶことが可能である．y の代表元 $\boldsymbol{t}$ についても同様である．

ノイズが，Pauli 通信路で与えられた場合，誤り $\vec{s} = (\boldsymbol{s},\boldsymbol{t})$ がある確率 $\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s}) = \mathrm{P}^{\mathbb{X}^{2r}}(\boldsymbol{s},\boldsymbol{t})$ で起きると考えることができる．この場合，第 1 成分の誤り $\boldsymbol{s}$ は，計算基底に関する誤りであり，**ビット誤り**とよばれ，第 2 成分の誤り $\boldsymbol{t}$ は，計算基底の位相に関する誤りであり，**位相誤り**とよばれる．そのため，CCS 符号では，誤り訂正をビット誤りの誤り訂正と位相誤りの誤り訂正に分割して行うことができる．2 つの誤り $\boldsymbol{s},\boldsymbol{t}$ が独立であるとき，（すなわち，$\mathbb{X}^r$ 上の 2 つの分布 $\mathrm{P}^{\mathbb{X}_1^r}, \mathrm{P}^{\mathbb{X}_2^r}$ を用いて，確率 $\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s})$ が $\mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})\mathrm{P}^{\mathbb{X}_2^r}(\boldsymbol{t})$ と記述されるとき，）$x \in C_1^*, y \in C_2^*$ に対して，それぞれの代表元 $\boldsymbol{s}_x, \boldsymbol{t}_y$ を独立に選ぶと，量子通信路 $D \circ \Lambda_{\mathcal{H}_0}$ のエンタングルメント忠実度は

$$
\begin{aligned}
&F_e^2(D \circ \Lambda_{\mathcal{H}_0}) \\
&= \sum_{x \in \mathbb{X}^r/C_2^\perp} \sum_{y \in \mathbb{X}^r/C_1^\perp} \sum_{\boldsymbol{s}' \in C_1} \sum_{\boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}^{2r}}((\boldsymbol{s}_x,\boldsymbol{t}_y) + (\boldsymbol{s}',\boldsymbol{t}')) \\
&= \left(\sum_{x \in \mathbb{X}^r/C_2^\perp, \boldsymbol{s}' \in C_1} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}_x + \boldsymbol{s}') \right) \left(\sum_{y \in \mathbb{X}^r/C_1^\perp, \boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}_2^r}(\boldsymbol{t}_y + \boldsymbol{t}') \right)
\end{aligned}
$$

となる．そして，$\sum_{x \in \mathbb{X}^r/C_2^\perp, \boldsymbol{s}' \in C_1} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}_x + \boldsymbol{s}')$ は古典的符号化対 $C_1 \subset C_2^\perp$ の最尤復号を用いたとき，最大となる．$\sum_{y \in \mathbb{X}^r/C_1^\perp, \boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}_2^r}(\boldsymbol{t}_y + \boldsymbol{t}')$ についても同様である．そのため，単純に双方の古典的符号化対の最尤復号を組み合わせることで CSS 符号の最尤復号が構成できる．

一方，2 つの誤り $\boldsymbol{s},\boldsymbol{t}$ が独立でないとき，それぞれの代表元を独立に選択するよりも，相関させて選択する方が優れている．この場合，$\mathbb{X}_1^r$ の部分の周辺分布を $\mathrm{P}^{\mathbb{X}_1^r}$ とし，$\mathbb{X}_2^r$ の部分の条件付き分布を $\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\cdot|\boldsymbol{s})$ とすると，$\mathrm{P}^{\mathbb{X}^{2r}}(\boldsymbol{s},\boldsymbol{t}) = \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}|\boldsymbol{s})$ となる．したがって，復号化においては，初めに，$x \in \mathbb{X}^r/C_2^\perp$ の代表元 $\boldsymbol{s}_x \in x$ を決め，次に，x に依存して $y \in \mathbb{X}^r/C_1^\perp$ の代表元 $\boldsymbol{t}_{x,y} \in y$ を決める．

この場合，量子通信路 $D \circ \Lambda_{\mathcal{H}_0}$ のエンタングルメント忠実度は

$$
F_e^2(D \circ \Lambda_{\mathcal{H}_0})
$$

$$= \sum_{x \in \mathbb{X}^r/C_2^\perp} \sum_{y \in \mathbb{X}^r/C_1^\perp} \sum_{\boldsymbol{s}' \in C_1} \sum_{\boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}^{2r}}((\boldsymbol{s}_x, \boldsymbol{t}_{x,y}) + (\boldsymbol{s}', \boldsymbol{t}'))$$

$$= \sum_{x \in \mathbb{X}^r/C_2^\perp, \boldsymbol{s}' \in C_1} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}_x + \boldsymbol{s}') \left(\sum_{y \in \mathbb{X}^r/C_1^\perp, \boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}_{x,y} + \boldsymbol{t}' | \boldsymbol{s}_x + \boldsymbol{s}') \right)$$

となる．エンタングルメント忠実度の評価のためには，1からエンタングルメント忠実度を引いた値を扱う方が扱いやすい．なぜなら，この値は誤り確率に相当するからである．

以下，$\boldsymbol{t}_{x,y} \in y$ を以下の方法で x に依存して決める場合に注目する．$\boldsymbol{t}$ は分布 $\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\cdot|\boldsymbol{s}_x)$ にしたがうと判断して，$\boldsymbol{t}_{y:\boldsymbol{s}_x}$ と判断する．ただし，$\boldsymbol{t}_{y:\boldsymbol{s}} := \mathrm{argmax}_{\boldsymbol{t} \in y} \sum_{\boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t} + \boldsymbol{t}'|\boldsymbol{s})$ と定義した．したがって，

$$\begin{aligned}
&1 - F_e^2(D \circ \Lambda_{\mathcal{H}_0}) \\
&\le (1 - \sum_{x \in \mathbb{X}^r/C_2^\perp} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}_x)) \\
&\quad + \sum_{x \in \mathbb{X}^r/C_2^\perp} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}_x) \left(1 - \sum_{y \in \mathbb{X}^r/C_1^\perp, \boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}_{y:\boldsymbol{s}_x} + \boldsymbol{t}'|\boldsymbol{s}_x) \right) \\
&\le (1 - \sum_{x \in \mathbb{X}^r/C_2^\perp} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}_x)) \\
&\quad + \sum_{\boldsymbol{s} \in \mathbb{X}^r} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s}) \left(1 - \sum_{y \in \mathbb{X}^r/C_1^\perp, \boldsymbol{t}' \in C_2} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}_{y:\boldsymbol{s}} + \boldsymbol{t}'|\boldsymbol{s}) \right) \qquad (5.37)
\end{aligned}$$

を得る．このように，古典的な符号 $C_2^\perp$ と符号 $C_1^\perp/C_2$ の誤り確率の評価に帰着できる．

なお，CSS符号の場合，$N^\perp/N = (C_2^\perp \times C_1^\perp)/(C_1 \times C_2) = C_2^\perp/C_1 \times C_1^\perp/C_2$ となり，$\mathcal{J} = \{(\boldsymbol{s}_x, \boldsymbol{t}_{x,y})\}_{(x,y) \in N^*}$ となる．したがって，$\mathrm{P}\{\mathcal{J} + N\}^{N^\perp/N} = \mathrm{P}\{\mathcal{J} + N\}^{C_2^\perp/C_1 \times C_1^\perp/C_2}$ となる．したがって，$\mathcal{J}_{2,x} := \{\boldsymbol{t}_{x,y}\}$ とすると，

$$\mathrm{P}\{\mathcal{J} + N\}^{C_1^\perp/C_2}(0) = \sum_{[\boldsymbol{x}] \in \mathbb{X}_1^r/C_2^\perp} \mathrm{P}^{\mathbb{X}_1^r/C_2^\perp}([\boldsymbol{x}]) \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r/C_2^\perp}(\mathcal{J}_{2,[\boldsymbol{x}]} + C_2|[\boldsymbol{x}])$$

を得る．

5.3.4　漸近理論

上記では，$\mathbb{X}^{2r}$ 上の一般の確率分布 $P^{\mathbb{X}^{2r}}$ を用いて，Pauli 通信路が与えられている場合を扱った．以下では，$\mathbb{F}_q^2$ 上の確率分布 $P^{\mathbb{F}_q^2}$ の r 次の独立同一分布を用いて，Pauli 通信路が与えられる場合を扱う．古典系と同様に，r が無限大の極限を扱う理論は漸近理論とよばれる．漸近理論においては符号の系列を扱うことになる．以下では CSS 符号に注目するとする．この場合，ねじれ条件を満たす符号の対 (C_1, C_2) の系列 $\{(C_{1,r}, C_{2,r})\}$ を扱うことになる．漸近理論において重要となるのが，エンタングルメント忠実度の極限値と伝送される量子系の次元の漸近的振る舞いを表す伝送レートである．後者は，(5.36) より，伝送される量子系の次元が $\frac{|C_{1,r}^{\perp}|\cdot|C_{2,r}^{\perp}|}{|\mathbb{F}_q|^r}$ であるので，

$$\lim_{r\to\infty}\frac{1}{r}\log\frac{|C_{1,r}^{\perp}|\cdot|C_{2,r}^{\perp}|}{|\mathbb{F}_q|^r}=\lim_{r\to\infty}\frac{\log|C_{1,r}^{\perp}||C_{2,r}^{\perp}|}{r}-\log|\mathbb{F}_q| \tag{5.38}$$

で与えられる．一方，前者については，その極限値が 1 に収束することを要求する．

$\mathbb{F}_q^2$ の第 1 成分と第 2 成分を表す集合を $\mathbb{F}_{q,1}$, $\mathbb{F}_{q,2}$ と記すことにすると，

$$R_1>\frac{H(P^{\mathbb{F}_{q,1}})}{\log q},\quad R_2>\frac{H(P^{\mathbb{F}_{q,2}|\mathbb{F}_{q,1}})}{\log q} \tag{5.39}$$

となる R_1, R_2 を選び，r に対して k_1, k_2 を $k_1=\lfloor(1-R_1)r\rfloor$, $k_2=\lfloor(1-R_2)r\rfloor$ となるように選ぶ．そして，$C_{1,X,r}^{\perp}$ を補題 5.1.5 で与えられた q^{k_1-r}-ユニバーサル 2 となる符号化のアンサンブルとする．$C_{1,X,r}^{\perp}$ を与えることで，$C_{1,X,r}$ が自動的に決まる．さらに，補題 5.1.5 と補題 5.1.7 を組み合わせることで，$C_{1,X,r}\subset\mathbb{F}_q^r$ に対して，$(1,q^{k_2-r})$-二重ユニバーサル 2 となる符号化のアンサンブル $C_{2,X,r}^{\perp}$ を与える [113, 46]．このとき，$C_{1,X,r}^{\perp}$ の次元は k_1 であり，$C_{2,X,r}^{\perp}$ の次元は k_2 である．したがって，伝送できる量子系の次元は $q^{k_1+k_2-r}$ となり，伝送レートは $\log q(1-R_1-R_2)$ となる．

一方，定理 5.1.2 および定理 5.1.4 の証明と同じ議論から，(5.37) の右辺は以下のように評価できる．

$$\left(1-\sum_{x\in\mathbb{X}^r/C_2^{\perp}}P^{\mathbb{F}_{q,1}}(\boldsymbol{s}_x)\right)$$

$$+\sum_{\boldsymbol{s}\in\mathbb{X}^r} \mathrm{P}^{\mathbb{F}_{q,1}}(\boldsymbol{s})\left(1-\sum_{y\in\mathbb{X}^r/C_1^{\perp},\boldsymbol{t}'\in C_2} \mathrm{P}^{\mathbb{F}_{q,2}|\mathbb{F}_{q,1}}(\boldsymbol{t}_{y:\boldsymbol{s}}+\boldsymbol{t}'|\boldsymbol{s})\right)$$

$$\leq \min_{0\leq s\leq 1} q^{s(k_1-r)}e^{\phi(s:\mathrm{P}^{\mathbb{F}_{q,1}})}+\min_{0\leq s\leq 1} q^{s(k_2-r)}e^{\phi(s:\mathrm{P}^{\mathbb{F}_{q,2}|\mathbb{F}_{q,1}})}.$$

したがって，条件 (5.39) より，この値は r について指数的に 0 に収束する．したがって，以下の値の伝送レートが達成できる [30].

$$\log q - H(\mathrm{P}^{\mathbb{F}_{q,1}}) - H(\mathrm{P}^{\mathbb{F}_{q,2}|\mathbb{F}_{q,1}}) = \log q - H(\mathrm{P}^{\mathbb{F}_q^2}).$$

なお，この値はコヒーレント情報量 $I_c(\rho_{\mathrm{mix}}, \Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}])$ に一致する．

5.3.5 物理的構成

初めに，最も典型的な Stabilizer 符号を考えよう．量子系 $\mathcal{H}^{\otimes r}$ に $\mathbb{F}_q^{2r}$ の離散 Heisenberg 表現が与えられているとする．このとき，最初の第 k 成分にのみ値を持つ $\mathbb{F}_q^{2r}$ の部分群 N_k を考える．この部分群 N_k は自己直交部分群であるので，N_k を Stabilizer とする Stabilizer 符号が構成できる．このとき，$N_k^{\perp}$ は最初の第 r 成分と第 $r+k+1$ 成分から第 $2r$ 成分にのみ値を持つ $\mathbb{F}_q^{2r}$ の部分群となる．この Stabilizer 符号では量子系 $\mathcal{H}^{\otimes r}$ の最初の k 個のテンソル積成分が $|0\rangle^{\otimes k}$ となる部分空間が符号空間となる．以下，この部分空間を $|0\rangle^{\otimes k}\otimes\mathcal{H}^{\otimes r-k}$ と記す．この符号空間は $\mathcal{H}^{\otimes r-k}$ と同型となる．復号化については，最初の k 個のテンソル積空間を計算基底について測定し，各測定値に対応する $\mathbb{F}_q^{2r}/N^{\perp}=N^*$ の要素 x を得る．そして，その代表元 $\vec{s}_x$ に対応するユニタリ行列 $\mathsf{W}_{\mathbb{F}}^r(\vec{s}_x)$ の逆元を作用させることで，復号が完了する．

しかし，一般の自己直交部分群 N は上記のような単純な形ではない．N が $\mathbb{F}_q$ 上の部分ベクトル空間として与えられる場合については，以下に述べるように上記の議論に帰着できる．N の次元を k とすると，N, $N^{\perp}$ は N_k, $N_k^{\perp}$ と $\mathbb{F}_q$ 上の部分ベクトル空間として内積構造まで含めて同型となる．$\mathbb{F}_q^{2r}$ 上の内積構造を保存する線形写像の集合は $\mathrm{Sp}(2r,\mathbb{F}_q)$ である．したがって，$\mathrm{Sp}(2r,\mathbb{F}_q)$ の要素 g を適切に選ぶと，$gN_k=N$, $gN_k^{\perp}=N^{\perp}$ となる．すなわち，最初に，伝送したい状態を量子系 $\mathcal{H}^{\otimes r-k}$ の状態として準備し，ユニタリ行列 $\mathsf{S}_{\mathbb{F}}^r(g)$ を施すことで，符号化が完成する．復号化は，ユニタリ行列 $\mathsf{S}_{\mathbb{F}}^r(g)^{\dagger}$ を施し，上記と同じように，最初の k 個のテンソル積成分を測定し，代表元に

対応する測定を行うことで実現できる [25, 26].

さらに，CSS 符号の場合にはより具体的に符号化が構成できる．以下に典型的な CSS 符号を考える．$C_{1:k_1}$ を初めの k_1 成分にのみ値を持つ $\mathbb{F}_q^r$ の部分群とし，$C_{2:k_2}$ を最後の k_2 成分にのみ値を持つ $\mathbb{F}_q^r$ の部分群とする．このとき，符号空間は $|0\rangle^{\otimes k_1} \otimes \mathcal{H}^{\otimes r-k_1-k_2} \otimes |0\rangle^{\otimes k_2}$ と記すことができる．そして，最初の k_1 個のテンソル積空間と最後の k_2 個のテンソル積空間を測定し，適切なユニタリ行列を施すことで復号化が可能となる．

一般のねじれ条件を満たす $\mathbb{F}_q^r$ の部分ベクトル空間の組 C_1, C_2 から決まる CSS 符号の符号化は以下のように構成できる．C_1, C_2 の次元を k_1, k_2 とする．符号 C_1 の $k_1 \times r$ の生成行列 γ_1 とし，これに，$(r-k_1-k_2)\times r$ 行列 γ_2 を加えて，2 つの行列を並べた $\gamma_1\gamma_2$ が $(r-k_2)\times r$ の符号 $C_2^\perp$ の生成行列となるようにする．最後に $k_2 \times r$ の行列 γ_3 を付け加えて $\gamma := \gamma_1\gamma_2\gamma_3$ が $\mathrm{GL}(r, \mathbb{F}_q)$ の要素となるようにする．このとき，$(\gamma^{-1})^T$ を同じように $\beta_1\beta_2\beta_3$ と分割すると β_3 は符号 C_2 の生成行列となる．この事実は $\gamma_1\gamma_2$ の $r-k_2$ 個の列ベクトルが β_3 の k_2 個の列ベクトルと直交することからわかる．同様に，$(r-k_1)\times r$ の行列 $\beta_2\beta_3$ は符号 $C_1^\perp$ の生成行列となる．したがって，計算基底に対しては，γ を施し，双対計算基底に対しては，$(\gamma^{-1})^T$ を施すことができれば，CSS 符号の符号化が可能となる．具体的には，[37] の (7.34) で定義したユニタリ行列 $\mathsf{S}_{\mathbb{F}}^r(M_\gamma)$ を作用させれば符号化が可能となる．（[37] の (7.35) に続く文を参照.）復号化については，ユニタリ行列 $\mathsf{S}_{\mathbb{F}}^r(M_\gamma)^\dagger$ を作用させ最初の k_1 成分については計算基底について測定し，最後の k_2 成分については双対計算基底について測定し，それぞれの測定値 x, y に応じて，代表元 $\boldsymbol{s}_{x,y} \in \mathbb{F}_{q,1}^r, \boldsymbol{t}_{x,y} \in \mathbb{F}_{q,2}^r$ を上記の議論に従って決め，その逆元に対応するユニタリを施すことになる．具体的には，$\mathsf{W}_{\mathbb{F}}^r(\gamma \boldsymbol{s}_{x,y}, 0)$, $\mathsf{W}_{\mathbb{F}}^r(0, (\gamma^{-1})^T \boldsymbol{t}_{x,y})$ を施すことで，復号化ができる．

したがって，CSS 符号の符号化および復号化は $\mathrm{GL}(r, \mathbb{F}_q)$ の作用および離散 Heisenberg 群の作用だけで実現できる [27].

一方，$\mathbb{X} = \mathbb{Z}_d$ の場合について考えてみよう．Stabilizer 符号の場合，N が可換群として，$\mathbb{Z}_d^k$ と同型である場合は，N_k を N に変換する　$\mathrm{Sp}(2r, \mathbb{Z}_d)$ の要素があるため，$\mathbb{F}_q$ の場合と同じ議論が可能となる．CSS 符号についても，C_1, C_2 がねじれ条件を満たし，それぞれが，$\mathbb{Z}_d^{k_1}$, $\mathbb{Z}_d^{k_2}$, と同型であれば，同じように，符号 C_1, $C_2^\perp$ の生成行列がとれる．そのため，$\mathbb{F}_q$ の場合と同じ議論

が可能となる．

5.4 Clifford 符号*

代数的な構造を持つ量子誤り訂正符号は，上述の Stabilizer 符号に限られない．より一般には，正規部分群 N を持つ群 G の既約ユニタリ表現が与えられた場合に構成できる．そのような符号は Clifford 符号とよばれる [77, 74, 75]．以下，Clifford 符号の定義のために必要な準備を行う．

$\hat{N}(\mathsf{f})$ を $\mathcal{H}$ に現れる N の既約ユニタリ表現のラベルの集合とし，$\lambda \in \hat{N}(\mathsf{f})$ に対して，**慣性群** $T(N, \lambda)$ を以下で定義する．（慣性群については，[37, 2.5.2 項] を参照のこと．）

$$T(N, \lambda) := \{g \in G \,|\, \chi_\lambda(gng^{-1}) = \chi_\lambda(n), \quad \forall n \in N\}. \tag{5.40}$$

すると，正規部分群 N の既約分解について以下の定理を得る．

定理 5.4.1　量子系 $\mathcal{H}$ に群 G の既約ユニタリ表現 f が与えられたとする．G の正規部分群 N の既約分解は以下で与えられる．

$$\mathcal{H} = \bigoplus_{\lambda \in \hat{N}(\mathsf{f})} \mathcal{U}_\lambda \oplus \mathbb{C}^m. \tag{5.41}$$

そして，$\mathcal{H}$ の部分空間 $\mathcal{K}_\lambda := \mathcal{U}_\lambda \oplus \mathbb{C}^m$ は $T(N, \lambda)$ の表現について既約な部分空間となる．さらに，上の分解に現れる $\mathcal{U}_\lambda$ の次元は全て等しく，$\mathcal{K}_\lambda$ への射影 $P(\mathcal{K}_\lambda)$ は以下のように表せる．

$$P(\mathcal{K}_\lambda) = \frac{\chi_\lambda(e)}{|N|} \sum_{n \in N} \chi_\lambda(n^{-1}) \mathsf{f}(n). \tag{5.42}$$

証明.　最初に N についての既約分解 $\mathcal{H} = \bigoplus_{\lambda \in \hat{N}(\mathsf{f})} \mathcal{U}_\lambda \oplus \mathbb{C}^{m_\lambda}$ を与える．そして，$\lambda \in \hat{N}(\mathsf{f})$ に対して，$\mathcal{K}_\lambda := \mathcal{U}_\lambda \oplus \mathbb{C}^{m_\lambda}$ を考える．$g \in T(N, \lambda)$ に注目する．指標から表現が一意に決まることから，$n \in N$ について，$n \mapsto \mathsf{f}_\lambda(gng^{-1})$ は $\mathsf{f}_\lambda(n)$ と同じ表現を与える．したがって，$\mathsf{f}_\lambda(n) = \mathsf{f}_\lambda(gng^{-1})$ となる．よって，$\mathsf{f}(g)\mathcal{U}_\lambda$ の要素を $\mathsf{f}(g)|u\rangle$ とすると，

$$\mathsf{f}(n)\mathsf{f}(g)|u\rangle = \mathsf{f}(g)\mathsf{f}(g^{-1})\mathsf{f}(n)\mathsf{f}(g)|u\rangle = \mathsf{f}(g)\mathsf{f}(g^{-1}ng)|u\rangle$$

$$= \mathsf{f}(g)\mathsf{f}_\lambda(g^{-1}ng)|u\rangle = \mathsf{f}(g)\mathsf{f}_\lambda(n)|u\rangle$$

となる．Schur の補題より，$\mathsf{f}(g)\mathcal{U}_\lambda$ での N の表現は，f_λ と同値である．一方，次に $g \in G \setminus T(N,\lambda)$ を選ぶ．すると，$n \mapsto \mathsf{f}_{g(\lambda)}(n) := \mathsf{f}_\lambda(gng^{-1})$ は $\mathsf{f}_\lambda(n)$ と異なる表現を与える．

$$\mathsf{f}(n)\mathsf{f}(g)|u\rangle = \mathsf{f}(g)\mathsf{f}(g^{-1})\mathsf{f}(n)\mathsf{f}(g)|u\rangle = \mathsf{f}(g)\mathsf{f}(g^{-1}ng)|u\rangle = \mathsf{f}(g)\mathsf{f}_{g(\lambda)}(n)|u\rangle$$

となるため，$\mathsf{f}(g)\mathcal{U}_\lambda$ での N の表現は，$\mathsf{f}_{g(\lambda)}$ となる．$\mathsf{f}_{g(\lambda)}$ の表現空間の次元は $\mathcal{U}_\lambda$ と同じである．したがって，$\hat{N}(\mathsf{f})$ に含まれる既約ユニタリ表現の次元は等しい．

また，$\mathsf{f}(g)$ は $\mathcal{K}_\lambda$ を $\mathcal{K}_{g(\lambda)}$ に移し，$\mathsf{f}(g^{-1})$ は $\mathcal{K}_{g(\lambda)}$ を $\mathcal{K}_\lambda$ に移すことから，$\mathcal{K}_\lambda$ の次元も $\lambda \in \hat{N}(\mathsf{f})$ に依存しない．したがって，m_λ も $\lambda \in \hat{N}(\mathsf{f})$ に依存しない．

ここで，$\mathcal{U}_\lambda$ を $T(N,\lambda)$ の作用に関する既約部分空間に含まれるように選ぶ．すると，$\{\mathsf{f}(g)\mathcal{U}_\lambda\}_{g\in G}$ は $\mathcal{H}$ を生成する．そして，

$$\{\mathsf{f}(g)\mathcal{U}_\lambda\}_{g\in T(N,\lambda)} = \{\mathsf{f}(g)\mathcal{U}_\lambda\}_{g\in G} \cap \mathcal{K}_\lambda = \mathcal{K}_\lambda$$

となり，$\mathcal{K}_\lambda$ は $T(N,\lambda)$ の作用に関して既約となる．さらに，(5.42) は [37] の (2.47) より得られる． □

さらに，等質空間 $G/T(N,\lambda)$ の要素 $[g] = gT(N,\lambda)$ に対して，$\mathsf{f}(g)\mathcal{K}_\lambda = \mathcal{K}_{g(\lambda)}$ とすると，$g(\lambda)$ は剰余類の代表元のとり方に依存しないので，$g(\lambda)$ を $[g](\lambda)$ と記す．したがって，S と等質空間 $G/T(N,\lambda)$ と同一視できる．$g' \in T(N,[g]\lambda)$ について，

$$\mathsf{f}(gg'g^{-1})\mathsf{f}(g)\mathcal{K}_\lambda = \mathsf{f}(g)\mathsf{f}(g')\mathsf{f}(g^{-1})\mathsf{f}(g)\mathcal{K}_\lambda = \mathsf{f}(g)\mathsf{f}(g')\mathcal{K}_\lambda = \mathsf{f}(g)\mathcal{K}_\lambda$$

となることから，$gT(N,\lambda)g^{-1} \subset T(N,[g]\lambda)$ を得る．逆の議論を考えることで，

$$gT(N,\lambda)g^{-1} = T(N,[g]\lambda) \tag{5.43}$$

を得る．一方，$g \in C(N)$ は Schur の補題より，各 $\mathcal{K}_\lambda$ 上で $\mathsf{f}(g)$ は定数となる．

したがって，ここで与えた構造を用いて，量子誤り訂正符号を構成することができる．初めに $\lambda \in \hat{N}(\mathsf{f})$ を1つ選び，$\mathcal{K}_\lambda$ を符号空間とする．そして，等質空間 $G/T(N,\lambda)$ の要素 x に対して，代表元 g_x を選ぶことで，以下のように復号化 D が構成できる．

$$D(\rho) := \sum_{x \in G/T(N,\lambda)} (P_{x(\lambda)}\mathsf{f}(g_x))^\dagger \rho P_{x(\lambda)}\mathsf{f}(g_x).$$

ここで与えた符号空間，復号化の組を **Clifford 符号**という [74, 75]．正規部分群 N を**符号の生成群**という．このとき，部分集合 $\{g_x\}C(N)$ の要素が働いたときには，完全に復元できる．すなわち，P を G の部分集合 $\{g_x\}C(N)$ にのみ値を持つ確率分布とし，量子通信路 $\Lambda[\mathrm{P}]$ を

$$\Lambda[\mathrm{P}](\rho) := \sum_{g \in \{g_x\}C(N)} \mathrm{P}(g)\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger$$

で定義すると，エンタングルメント忠実度 $F_e^2(D \circ \Lambda[\mathrm{P}])$ は1となる．

また，$|x\rangle \in \mathcal{U}_\lambda$ に対して，$|x\rangle \otimes \mathbb{C}^m \subset \mathcal{K}_\lambda$ を符号空間とし，復号化 D を

$$D(\rho) := \mathrm{Tr}_{\mathcal{U}_\lambda} \sum_{x \in G/T(N,\lambda)} (P_{x(\lambda)}\mathsf{f}(g_x))^\dagger \rho P_{x(\lambda)}\mathsf{f}(g_x)$$

とする量子誤り訂正符号を考えることができる．この符号を **Subsystem 符号**とよぶ [76]．このとき，部分集合 $\{g_x\}N$ の要素が働いたときには，完全に復元できる．すなわち，P を G の部分集合 $\{g_x\}N$ にのみ値を持つ確率分布とし，量子通信路 $\Lambda[\mathrm{P}]$ を

$$\Lambda[\mathrm{P}](\rho) := \sum_{g \in \{g_x\}N} \mathrm{P}(g)\mathsf{f}(g)\rho\mathsf{f}(g)^\dagger$$

で定義すると，エンタングルメント忠実度 $F_e^2(D \circ \Lambda[\mathrm{P}])$ は1となる．

以下いくつか重要な性質を列挙する．

補題 5.4.2　N が G の正規部分群であるとき，以下が成り立つ．

(1) N の中心 $C(N)$ は G の正規部分群となる．

(2) G の既約ユニタリ表現 f と，$\lambda \in \hat{N}(\mathsf{f})$ に対し，$C_G(N) \subset T(N,\lambda)$ となる．

証明. $n \in C(N), n' \in N, g \in G$ について，$gn'g^{-1}n = ngn'g^{-1}$ となる．左から g^{-1} を掛け，右から g を掛けると $n'g^{-1}ng = g^{-1}ngn'$ を得る．よって，$g^{-1}ng \in C(N)$ となり，$C(N)$ は G の正規部分群となる．

そして，$g \in C_G(N), n \in N$ に対し，$\mathsf{f}_\lambda(g^{-1}ng) = \mathsf{f}_\lambda(n)$ となることから，$g \in T(N,\lambda)$ となる． □

補題 5.4.3 $[G,G] \subset C(G)$ であるとする．G の既約ユニタリ表現 f に対し，以下が成り立つ．

(1) $\lambda \in \hat{N}(\mathsf{f})$ について $T(N,\lambda)$ は G の正規部分群となる．そのため (5.43) より，$T(N,\lambda)$ は $\lambda \in \hat{N}(\mathsf{f})$ の選び方に依存しない．以下 $T(N,\lambda)$ を $T(N,\mathsf{f})$ と記す．

(2) $T(N,\mathsf{f})$ についての慣性群は $T(N,\mathsf{f})$ である．

(3) $N_1 \subset N_2$ となる 2 つの G の正規部分群が与えられたとき，$T(N_2,\mathsf{f}) \subset T(N_1,\mathsf{f})$ となる．

証明. $g' \in T(N,\lambda), n \in N, g \in G$ に対して，$a := gg'g^{-1}g'^{-1} \in C(G)$ とすると，$gg'g^{-1} = ag'$ となるので，

$$gg'g^{-1}ngg'^{-1}g^{-1} = ag'ngg'^{-1}g^{-1} = g'ngg'^{-1}g^{-1}a = g'ng'^{-1}$$

となり，$\chi_\lambda(gg'g^{-1}ngg'^{-1}g^{-1}) = \chi_\lambda(g'ng'^{-1}) = \chi_\lambda(n)$ を得る．よって，$gg'g^{-1} \in T(N,\lambda)$ となり，$T(N,\lambda)$ は G の正規部分群となる．

異なる $\lambda, \lambda' \in \hat{N}(\mathsf{f})$ について，$T(N,\mathsf{f})$ の $\mathcal{K}_\lambda$ への表現は $\mathcal{K}_{\lambda'}$ への表現と異なる．この事実は部分群 N の要素の表現を考えれば自明である．したがって，$G \setminus T(N,\mathsf{f})$ には $T(N,\mathsf{f})$ の慣性群の要素は含まれない．よって (2) を得る．

$T(N_1,\mathsf{f})$ の要素となる条件と $T(N_2,\mathsf{f})$ の要素となる条件を比較すると (3) を得る． □

補題 5.4.4 $[G,G] \subset C(G)$ であるとする．G の $\mathcal{H}$ 上の既約ユニタリ表現 f が $C(G)$ において忠実であるとする．すなわち，$\mathsf{f}(g) \neq I$ となる $g \in C(G)$ は単位元に限られるとする．このとき以下が成り立つ．

(1) $\dim \mathcal{H}^2 = \frac{|G|}{|C(G)|}$.

(2)　G の正規部分群 N は $T(N,\mathsf{f}) = C_G(C(N))$ を満たす.

(3)　G の正規部分群 N は $T(N,\mathsf{f}) = T(C(N),\mathsf{f})$ を満たす.

(4)　$C(N_2) \subset N_1 \subset N_2$ となる 2 つの G の正規部分群が与えられたとき, $T(N_2,\mathsf{f}) = T(N_1,\mathsf{f})$ となる.

(5)　$\lambda \in \hat{N}(\mathsf{f})$ について以下が成り立つ.

$$\dim \mathcal{K}_\lambda = \frac{|C(G) \cap N|}{|N|} \dim \mathcal{H}_\lambda^2 \dim \mathcal{H}, \tag{5.44}$$

$$\dim \mathcal{H}_\lambda^2 = \frac{|N|}{|C(N)|}. \tag{5.45}$$

証明.　最後に **(1)** を示す.

(2) の証明：補題 5.4.2 の **(2)** より, $T(N,\mathsf{f}) \subset C_G(C(N))$ を示せば十分である. $\lambda \in \hat{N}(\mathsf{f})$ と $g \in T(N,\mathsf{f})$ に対して, $n \in C(N)$ を選ぶと, $a := gng^{-1}n^{-1} \in [G,G] \subset C(G)$ となり, $\mathsf{f}_\lambda(a)$ は定数 ω となる. $g \in T(N,\mathsf{f})$ であるから,

$$\chi_\lambda(n) = \chi_\lambda(gng^{-1}) = \chi_\lambda(an) = \omega\chi_\lambda(n)$$

を得る. [37] の補題2.3.4 より, $n \in \mathrm{supp}(\chi_\lambda)$ となる. したがって, $\omega = 1$ となる. この事実は条件より, $gng^{-1}n^{-1} = e$ を意味する. よって, $g \in C_G(C(N))$ となり **(2)** を得る.

(3) の証明：**(2)** の N に $C(N)$ を代入すると, $T(C(N),\mathsf{f}) = C_G(C(N))$ となり, **(3)** を得る.

(4) の証明：補題 5.4.3 より, $T(N_2,\mathsf{f}) \subset T(N_1,\mathsf{f}) \subset T(C(N_2),\mathsf{f})$ となる. **(2)** より, **(4)** を得る.

(5) の証明：$\dim \mathcal{K}_\lambda = \mathrm{Tr}\, P(\mathcal{K}_\lambda)$ であるので, 定理 5.4.1 の (5.42) の右辺のトレースを求める. N の要素で $\mathrm{Tr}\, \mathsf{f}(n)$ が 0 でないものは, $C(G)$ に含まれるものに限られる ([37, 補題 2.3.3] を参照のこと). $n \in N \cap C(G)$ については, $\mathsf{f}(n)$ および, $\mathsf{f}_\lambda(n)$ は単位行列の同じ定数 ω 倍となる. したがって, $\chi_\lambda(n^{-1})\mathsf{f}(n) = \dim \mathcal{U}_\lambda I_{\mathcal{H}}$ となる. したがって, 定理 5.4.1 の (5.42) より,

$$\mathrm{Tr}\, P(\mathcal{K}_\lambda) = \frac{\chi_\lambda(e)}{|N|} \sum_{n \in N \cap C(G)} \dim \mathcal{U}_\lambda \dim \mathcal{H} = \frac{|C(G) \cap N|}{|N|} \dim \mathcal{H}_\lambda^2 \dim \mathcal{H}$$

となり，(5.44) を得る．

さらに，$C(N)$ を符号の生成群とする場合も，慣性群は同じであり，$\mathcal{K}_\lambda$ は慣性群 $T(C(N),\mathsf{f})$ の表現に関して既約である．したがって，$C(N)$ を符号の生成群とする場合に (5.44) を適用すると，

$$\operatorname{Tr} P(\mathcal{K}_\lambda) = \frac{|C(G) \cap C(N)|}{|C(N)|} \dim \mathcal{H} \tag{5.46}$$

を得る．$C(G) \cap C(N) = C(G) \cap N$ であるから，(5.44) と (5.46) を比較すると，(5.45) を得る．

(1) の証明：$C(G)$ を符号の生成群とする場合に (5.45) を適用すると，**(1)** を得る． □

Stabilizer 符号は以下のように Clifford 符号の特殊例と見なせる．群 G として，離散 Heisenberg 群 $\mathrm{H}(\mathbb{X}, 2r)$ を考える．$\mathbb{X}^r$ の自己直交群 N を考え，$C(\mathrm{H}(\mathbb{X}, 2r))$ の N による拡大を符号の生成群となる正規部分群とする．すると，N に基づく Stabilizer 符号は Clifford 符号となる．

一方，Subsystem 符号は半直積群 $H \rtimes K$ の以下の既約ユニタリ表現が与えられたときには有効である．H の既約ユニタリ表現 f_H, K の既約ユニタリ表現 f'_K と K のユニタリ表現である f_H の随伴表現 f_K が与えられたとき，半直積群 $H \rtimes K$ の既約ユニタリ表現 $\mathsf{f}_H \rtimes \mathsf{f}_K \otimes \mathsf{f}'_H$ が定義できる．この表現の下で，正規部分群 H を符号の生成群とすると，K の既約ユニタリ表現 f'_K の表現空間が符号空間となる．この場合，H の表現が 1 種類しかないので，代表元の選択はなく，復号化 D は f_H の表現空間についての部分トレースとして与えられる．

そして，ノイズを表す量子通信路が H 上の確率分布 P を用いて，$\Lambda[\mathrm{P}]$ で与えられているとき，$D \circ \Lambda[\mathrm{P}]$ のエンタングルメント忠実度は 1 となる．

例 5.4.5 群 $\mathrm{H}(2r, \mathbb{F}_q) \rtimes \mathrm{Sp}(2r, \mathbb{F}_q)$ のユニタリ表現 $(\mathsf{W}^r_{\mathbb{F},\mathrm{H}} \rtimes \mathsf{S}^r_{\mathbb{F}})^{\otimes 2}$ を考え，その既約成分 $\mathcal{H}_s$ に注目する．（具体的な表現の定義については [37] の 7.3.3 項を参照．）ただし，q は奇数とする．

[37] の (7.39) で与えられる既約分解より，符号空間は $\mathbb{C}^{(q^r+1)/2}$ となる．このとき，正規部分群である $\mathrm{H}(2r, \mathbb{F}_q)$ の任意の要素が働いても完全に復元できる．すなわち，$\mathcal{H}^{\otimes r}$ と同じ次元の量子系が 2 つ準備され，ノイズとして働く．

$\mathsf{W}_{\mathbb{F}}^r(\vec{s})$ は2つの空間で同じユニタリが働く場合には，空間 $\mathbb{C}^{(q^r+1)/2}$ にはノイズは働かない．

この量子誤り訂正符号は仮定しているノイズが特殊ではあるが，このような特殊なノイズの下では極めて有効である．

5.5　エンタングルメント蒸留と一般の通信路への適用

上記の議論では，Pauli 通信路に限った議論を行っていた．しかし，上記の議論は一般の通信路へ拡張可能である．そのために，量子誤り訂正のエンタングルメント蒸留への応用を扱う [5, 106, 84]．量子系 $\mathcal{H}_B \otimes \mathcal{H}_A := (\mathcal{H}^{\otimes r})^{\otimes 2}$ 上の一般の状態 ρ が与えられたとき，$\mathbb{X}^{2r}$ の部分群 N と $N^* = \mathbb{X}^{2r}/N^{\perp}$ の要素の代表元の集合 $\mathcal{J} := \{\vec{s}_x\}_{x \in N^*}$ を用いて，以下の LOCC 操作による**エンタングルメント蒸留**のプロトコルが与えられる．このプロトコルでは，$\mathcal{H}_0^{\otimes 2}$ 上の最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}_0}}|P_0\rangle\rangle$ に近い状態を生成する．

$$
\begin{aligned}
&\Lambda_{dis}[N, \mathcal{J}](\rho) \\
&:= \sum_{x, x' \in N^*} (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x-x'}) \otimes I)^\dagger (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) \otimes \overline{\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})})^\dagger (P_x \otimes P_{x'}^T) \\
&\quad \cdot \rho (P_x \otimes \overline{P_{x'}}) (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) \otimes \overline{\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})}) (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x-x'}) \otimes I) \\
&= \sum_{x, x' \in N^*} (P_0 \otimes P_0^T) (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) \otimes \overline{\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})})^\dagger (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x-x'}) \otimes I)^\dagger \\
&\quad \cdot \rho (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x-x'}) \otimes I) (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) \otimes \overline{\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})}) (P_0 \otimes \overline{P_0}).
\end{aligned} \tag{5.47}
$$

ここで，(5.47) は (5.35) から得られる．このとき，P_0 の値域は $\mathcal{H}_0$ であるので，終状態は $\mathcal{H}_0^{\otimes 2}$ 上の状態となる．(5.35) より，$\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) P_0 \mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})^\dagger = P_{x'}$ となるから，$\mathcal{H}_0^{\otimes 2}$ 上の最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}_0}}|P_0\rangle\rangle$ は以下を満たす．

$$
\begin{aligned}
&\frac{1}{\dim \mathcal{H}_0} \sum_{x' \in N^*} (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) \otimes \overline{\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})}) (P_0 \otimes \overline{P_0}) |P_0\rangle\rangle\langle\langle P_0| \\
&\quad \cdot (P_0 \otimes P_0^T) (\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'}) \otimes \overline{\mathsf{W}_{\mathbb{X}}^r(\vec{s}_{x'})})^\dagger \\
&\qquad = \frac{1}{\dim \mathcal{H}_0} \sum_{x' \in N^*} |P_{x'}\rangle\rangle\langle\langle P_{x'}|
\end{aligned}
$$

$$= \frac{1}{\dim \mathcal{H}^{\otimes r}} \sum_{\vec{s} \in N} |\mathsf{W}^r_{\mathbb{X}}(\vec{s})\rangle\rangle\langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s})|.$$

最後の式は $\sum_{\vec{s} \in N} \omega_{\mathbb{X}}^{x'(\vec{s})} = 0$ であることと $x' \neq 0$ であることの同値性に加え，[37] の (7.21) から得られる $|\mathsf{W}^r_{\mathbb{X}}(\vec{s})\rangle\rangle = \sum_{x' \in N^*} \omega_{\mathbb{X}}^{x'(\vec{s})} |P_{x'}\rangle\rangle$ を用いると示すことができる．

したがって，$x - x'$ を新たに，x とおくと，上の2つの式より，

$$\begin{aligned}
&\frac{1}{\dim \mathcal{H}_0} \Lambda_{dis}[N, \mathcal{J}]^*(|P_0\rangle\rangle\langle\langle P_0|) \\
&= \frac{1}{\dim \mathcal{H}^{\otimes r}} \sum_{x \in N^*} (\mathsf{W}^r_{\mathbb{X}}(\vec{s}_x) \otimes I) \sum_{\vec{s} \in N} |\mathsf{W}^r_{\mathbb{X}}(\vec{s})\rangle\rangle\langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s})| (\mathsf{W}^r_{\mathbb{X}}(\vec{s}_x) \otimes I)^\dagger \\
&= \frac{1}{\dim \mathcal{H}^{\otimes r}} \sum_{x \in N^*} \sum_{\vec{s} \in N} |\mathsf{W}^r_{\mathbb{X}}(\vec{s} + \vec{s}_x)\rangle\rangle\langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s} + \vec{s}_x)|
\end{aligned}$$

を得る．

すなわち，右辺は復号可能な誤りに対応する純粋状態 $|\mathsf{W}^r_{\mathbb{X}}(\vec{s} + \vec{s}_x)\rangle\rangle$ から生成される射影空間となる．以下，この射影空間を $P_{[N,\mathcal{J}]}$ と記す．ゆえに，$\Lambda_{dis}[N, \mathcal{J}](\rho)$ と最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}_0}} |P_0\rangle\rangle$ との忠実度は

$$\begin{aligned}
&\langle\langle P_0 | \Lambda_{dis}[N, \mathcal{J}](\rho) | P_0\rangle\rangle = \mathrm{Tr}\, \rho \frac{1}{\dim \mathcal{H}_0} \Lambda_{dis}[N, \mathcal{J}]^*(|P_0\rangle\rangle\langle\langle P_0|) \\
&\quad = \mathrm{Tr}\, \rho P_{[N,\mathcal{J}]} = \sum_{x \in N^*} \sum_{\vec{s} \in N} \frac{1}{\dim \mathcal{H}^{\otimes r}} \langle\langle \mathsf{W}^r_{\mathbb{X}}(\vec{s} + \vec{s}_x) | \rho | \mathsf{W}^r_{\mathbb{X}}(\vec{s} + \vec{s}_x)\rangle\rangle
\end{aligned}$$

で与えられる．

量子系 $\mathcal{H}_C \otimes \mathcal{H}_A := (\mathcal{H}^{\otimes r})^{\otimes 2}$ 上の最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}^{\otimes r}}} |I\rangle\rangle$ に準備し，出力系を系 $\mathcal{H}_B$ とする一般の通信路 Λ を用いて系 $\mathcal{H}_C$ を伝送したとする．この手法で得られる状態に LOCC プロトコル $\Lambda_{dis}[N, \mathcal{J}]$ を施したときの終状態と最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}_0}} |P_0\rangle\rangle$ との忠実度は以下のように計算できる．以下では，上記の議論に加え，例 4.4.4 で述べた $P[\Lambda](\mathcal{J} + N)$ の定義や twirling の結果得られる通信路 $\overline{\Lambda}_{\mathbb{X}^{2r}}$ に関する議論を用いた．

$$\frac{1}{\dim \mathcal{H}^{\otimes r} \dim \mathcal{H}_0} \langle\langle P_0 | \Lambda_{dis}[N, \mathcal{J}] \circ (\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|) | P_0\rangle\rangle$$

$$
\begin{aligned}
&= \mathrm{Tr}\,\frac{1}{\dim \mathcal{H}^{\otimes r}}(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)P_{[N,\mathcal{J}]} \\
&= \sum_{x \in N^*} \sum_{\vec{s} \in N} \frac{1}{\dim \mathcal{H}_A^2} \langle\langle \mathsf{W}_{\mathbb{X}}^r(\vec{s} + \vec{s}_x)|(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)|\mathsf{W}_{\mathbb{X}}^r(\vec{s} + \vec{s}_x)\rangle\rangle \\
&= P[\Lambda](\mathcal{J} + N) \qquad (5.48) \\
&= \sum_{x \in N^*} \sum_{\vec{s} \in N} \frac{1}{\dim \mathcal{H}_A^2} \langle\langle \mathsf{W}_{\mathbb{X}}^r(\vec{s} + \vec{s}_x)|(\overline{\Lambda}_{\mathbb{X}^{2r}} \otimes id)(|I\rangle\rangle\langle\langle I|)|\mathsf{W}_{\mathbb{X}}^r(\vec{s} + \vec{s}_x)\rangle\rangle.
\end{aligned}
$$

初期状態が最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}^{\otimes r}}}|I\rangle\rangle$ であり，量子操作 $(\Lambda \otimes id)$ を行ったとき，系 $\mathcal{H}_A$ で測定 $\{P_{x'}\}_{x' \in N^*}$ を行う代わりに，確率 $\frac{1}{|N|}$ で初期状態 $|P_{x'}\rangle\rangle$ を生成しても同じである．すなわち，

$$
\begin{aligned}
&\frac{1}{\dim \mathcal{H}^{\otimes r}} \sum_{x \in N^*} (I \otimes P_x^T)(\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)(I \otimes P_x^T) \\
&\quad = \frac{1}{\dim \mathcal{H}_0} \frac{1}{|N|} \sum_{x \in N^*} (\Lambda \otimes id)(|P_x\rangle\rangle\langle\langle P_x|) \qquad (5.49)
\end{aligned}
$$

が成り立つ．さらに，

$$
\Lambda_{dis}[N, \mathcal{J}]\left(\sum_{x \in N^*} (I \otimes P_x^T)\rho(I \otimes P_x^T) \right) = \Lambda_{dis}[N, \mathcal{J}](\rho) \qquad (5.50)
$$

が成り立つ．したがって，以下の式を得る．

$$
\begin{aligned}
&\sum_{x' \in N} \frac{1}{|N|} \frac{1}{\dim \mathcal{H}_0^2} \langle\langle P_0|\Lambda_{dis}[N, \mathcal{J}] \circ (\Lambda \otimes id)(|P_{x'}\rangle\rangle\langle\langle P_{x'}|)|P_0\rangle\rangle \\
&\quad = \frac{1}{\dim \mathcal{H}^{\otimes r} \dim \mathcal{H}_0} \langle\langle P_0|\Lambda_{dis}[N, \mathcal{J}] \circ (\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)|P_0\rangle\rangle \\
&\quad = P[\Lambda](\mathcal{J} + N). \qquad (5.51)
\end{aligned}
$$

ここで，第1式は (5.49), (5.50) から導かれ，第2式は (5.48) から導ける．さらに，$\Lambda_{dis}[N, \mathcal{J}]$ の定義から，

$$
\sum_{x' \in N} \frac{1}{|N|} \frac{1}{\dim \mathcal{H}_0^2} \langle\langle P_0|\Lambda_{dis}[N, \mathcal{J}] \circ (\Lambda \otimes id)(|P_{x'}\rangle\rangle\langle\langle P_{x'}|)|P_0\rangle\rangle
$$

$$= \sum_{x' \in N} \frac{1}{|N|} \frac{1}{\dim \mathcal{H}_0^2} \langle\langle P_{x'}|((D \circ \Lambda) \otimes id)(|P_{x'}\rangle\rangle\langle\langle P_{x'}|)|P_{x'}\rangle\rangle$$

$$= \sum_{x' \in N} \frac{1}{|N|} F_e^2(D \circ \Lambda|_{\mathcal{H}_{x'}}) \tag{5.52}$$

が成り立つ.

したがって, (5.51), (5.52) をまとめると以下の定理を得る.

定理 5.5.1 一般の量子通信路 Λ に対して, 表現 $\mathsf{W}_{\mathbb{X}}^r$ による twirling を $\Lambda[\mathsf{W}_{\mathbb{X}}, P]$ とする. 符号空間 $\mathcal{H}_x$ を N^* の一様分布に従って選んだ場合, 一般の量子通信路 Λ に対して, 誤り訂正 $\Lambda[N, \mathcal{J}]$ を施したときのエンタングルメント忠実度の平均値は $P(\mathcal{J} + N)$ となる.

上記の議論と同じようにして, $[\vec{s}] \in N^{\perp}/N$ によって定まる最大エンタングル状態 $\frac{1}{\sqrt{\dim \mathcal{H}_{x'}}}|\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_{x'}}([\vec{s}])\rangle\rangle$ との忠実度の平均値は以下のように計算できる.

$$\sum_{x' \in N} \frac{1}{|N|} \frac{1}{\dim \mathcal{H}_0^2} \langle\langle \mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_{x'}}([\vec{s}])|(D \circ \Lambda) \otimes id)(|P_{x'}\rangle\rangle\langle\langle P_{x'}|)|\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_{x'}}([\vec{s}])\rangle\rangle$$

$$= \sum_{x' \in N} \frac{1}{|N|} \frac{1}{\dim \mathcal{H}_0^2} \langle\langle \mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_0}([\vec{s}])|\Lambda_{dis}[N, \mathcal{J}]$$

$$\circ (\Lambda \otimes id)(|P_{x'}\rangle\rangle\langle\langle P_{x'}|)|\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_0}([\vec{s}])\rangle\rangle$$

$$= \frac{1}{\dim \mathcal{H}^{\otimes r} \dim \mathcal{H}_0} \langle\langle \mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_0}([\vec{s}])|\Lambda_{dis}[N, \mathcal{J}]$$

$$\circ (\Lambda \otimes id)(|I\rangle\rangle\langle\langle I|)|\mathsf{W}_{\mathbb{X}}^r|_{\mathcal{H}_0}([\vec{s}])\rangle\rangle$$

$$= P[\Lambda](\mathcal{J} + N + \vec{s}) = P[\Lambda]\{\mathcal{J} + N\}([\vec{s}]) \tag{5.53}$$

が成り立つ. ここで, 第1式は (5.52) と類似の議論から得られ, 第2式は (5.50), (5.49) と類似の議論から得られ, 第3式は (5.48) と類似の議論から得られる.

5.6 量子秘匿通信

5.6.1 秘匿性増強を行わない場合

量子系での通信では，単一の量子を使って通信するため誤りなくコヒーレンスを保ったまま受信者に量子状態を伝送することに成功すれば完全な秘匿通信に成功する [102]．盗聴者が情報を獲得するためには，送信信号との間に相互作用が必要である．しかし，コヒーレンスを保った通信に成功すると，他と相互作用のない通信に成功したことになり，完全な秘匿性が実現できる．以下では，個々の通信路がどれだけの秘匿性を持っているか定量的に議論するための枠組みを扱う．盗聴者がどれだけ環境系に漏れた情報を獲得しているかわからない．そのため，与えられた量子通信路 Λ の下，環境系へ漏れた情報が全て盗聴者に漏れたと考えて秘匿性の議論を行う．そのため，環境系への通信路 Λ_E を考え，その通信路の出力と入力系との相関を用いて盗聴者への情報漏洩を評価する．1つめの基準は，伝送情報量である．入力系で状態 $|x\rangle$ を確率 $P(x)$ で生成するときの伝送情報量は

$$
\begin{aligned}
I(P:\Lambda_E) &:= H\left(\Lambda_E\left(\sum_x P(x)|x\rangle\langle x|\right)\right) - \sum_x P(x)H(\Lambda_E(|x\rangle\langle x|)) \\
&= D(\rho_{A,E}\|\rho_A\otimes\rho_E).
\end{aligned}
$$

ここで，$\rho_{A,E}$, ρ_A, ρ_E を以下で定義した．

$$
\rho_{A,E} := \sum_x P(x)|x\rangle\langle x|\otimes\Lambda_E(|x\rangle\langle x|), \quad \rho_A := \mathrm{Tr}_E\,\rho_{A,E}, \quad \rho_E := \mathrm{Tr}_A\,\rho_{A,E}.
$$

他に，実際の合成系の状態 $\rho_{A,E}$ と相関がない場合ときの状態 $\rho_A\otimes\rho_E$ との差のトレースノルムを基準にとる場合がある．

$$
\begin{aligned}
d_1(P:\Lambda_E) &:= \|\rho_{A,E}-\rho_A\otimes\rho_E\|_1 \\
&= \sum_x P(x)\|\Lambda_E(|x\rangle\langle x|) - \Lambda_E(\sum_x P(x)|x\rangle\langle x|)\|_1. \qquad (5.54)
\end{aligned}
$$

さらに，トレースノルムの最大値を考えることで以下の基準を得る．

$$
d_{1,\max}(P:\Lambda_E) := \max_{x,x':P(x)>0}\|\Lambda_E(|x\rangle\langle x|) - \Lambda_E(|x'\rangle\langle x'|)\|_1.
$$

Pauli 通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]$ の環境系への通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]_E$ は (2.8) より，環境系の基底を $|\vec{s}\rangle$ とすると，以下で与えられる．

$$\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]_E(\rho) = \sum_{\vec{s},\vec{s}'} \sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s})}\sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s}')}[\mathrm{Tr}\, \mathsf{W}^r_{\mathbb{X}}(\vec{s})\rho \mathsf{W}^r_{\mathbb{X}}(-\vec{s}')]|\vec{s}\rangle\langle\vec{s}'|.$$

入力状態が計算基底 $|\boldsymbol{s}\rangle$ の場合, $\vec{s} = (\boldsymbol{s}, \boldsymbol{t})$ とすると, $\mathsf{W}^r_{\mathbb{X}}(\vec{s})|\boldsymbol{x}\rangle = \tau_{\mathbb{X}}^{\boldsymbol{s}\cdot\boldsymbol{t}}\omega_{\mathbb{X}}^{\boldsymbol{t}\cdot\boldsymbol{x}}|\boldsymbol{x} + \boldsymbol{s}\rangle$ となる．したがって，環境系への通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]_E$ の出力状態は以下で与えられる．

$$\begin{aligned}
&\Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]_E(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|) \\
&= \sum_{\vec{s},\vec{s}'} \sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s})}\sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\vec{s}')}\langle\boldsymbol{x}|\mathsf{W}^r_{\mathbb{X}}(-\vec{s}')\mathsf{W}^r_{\mathbb{X}}(\vec{s})|\boldsymbol{x}\rangle|\vec{s}\rangle\langle\vec{s}'| \\
&= \sum_{\boldsymbol{s},\boldsymbol{t},\boldsymbol{s}',\boldsymbol{t}'} \sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\boldsymbol{s},\boldsymbol{t})}\sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\boldsymbol{s}',\boldsymbol{t}')}\tau_{\mathbb{X}}^{\boldsymbol{s}\cdot\boldsymbol{t}-\boldsymbol{s}'\cdot\boldsymbol{t}'}\omega_{\mathbb{X}}^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}} \\
&\quad \cdot\langle\boldsymbol{x}+\boldsymbol{s}'|\boldsymbol{x}+\boldsymbol{s}\rangle|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s}',\boldsymbol{t}')| \\
&= \sum_{\boldsymbol{s},\boldsymbol{t},\boldsymbol{t}'} \sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\boldsymbol{s},\boldsymbol{t})}\sqrt{\mathrm{P}^{\mathbb{X}^{2r}}(\boldsymbol{s},\boldsymbol{t}')}\tau_{\mathbb{X}}^{(\boldsymbol{s}+2\boldsymbol{x})\cdot(\boldsymbol{t}-\boldsymbol{t}')}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t}')| \\
&= \sum_{\boldsymbol{s}} \mathrm{P}^{\mathbb{X}^r_1}(\boldsymbol{s})\sum_{\boldsymbol{t},\boldsymbol{t}'} \sqrt{\mathrm{P}^{\mathbb{X}^r_2|\mathbb{X}^r_1}(\boldsymbol{t}|\boldsymbol{s})}\sqrt{\mathrm{P}^{\mathbb{X}^r_2|\mathbb{X}^r_1}(\boldsymbol{t}'|\boldsymbol{s})}\tau_{\mathbb{X}}^{(\boldsymbol{s}+2\boldsymbol{x})\cdot(\boldsymbol{t}-\boldsymbol{t}')}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t}')| \\
&= \sum_{\boldsymbol{s}} \mathrm{P}^{\mathbb{X}^r_1}(\boldsymbol{s})\rho_{E,\boldsymbol{s}}(\boldsymbol{x}).
\end{aligned}$$

ここで，$\rho_{E,\boldsymbol{s}}(\boldsymbol{x}) := \sum_{\boldsymbol{t},\boldsymbol{t}'} \sqrt{\mathrm{P}^{\mathbb{X}^r_2|\mathbb{X}^r_1}(\boldsymbol{t}|\boldsymbol{s})}\sqrt{\mathrm{P}^{\mathbb{X}^r_2|\mathbb{X}^r_1}(\boldsymbol{t}'|\boldsymbol{s})}\tau_{\mathbb{X}}^{(\boldsymbol{s}+2\boldsymbol{x})\cdot(\boldsymbol{t}-\boldsymbol{t}')}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s}, \boldsymbol{t}')|$ とした．

補題 5.6.1 （エントロピーによる評価 [46, 89]）

$$I(P : \Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]_E) \le H(\mathrm{P}^{\mathbb{X}^r_2|\mathbb{X}^r_1}) \le H(\mathrm{P}^{\mathbb{X}^r_2}). \tag{5.55}$$

P が一様分布 P_{mix} のとき 1 つ目の不等式にて等号が成立する．したがって，(2.40) より，

$$I(P : \Lambda[\mathsf{W}^r_{\mathbb{X}}, \mathrm{P}^{\mathbb{X}^{2r}}]_E) \le (1 - \mathrm{P}^{\mathbb{X}^r_2}(0)) \log|\mathbb{X}^r| + h(\mathrm{P}^{\mathbb{X}^r_2}(0)) \tag{5.56}$$

を得る．

証明.　P が一様分布のとき $\rho_{E,\boldsymbol{s}}(\boldsymbol{x})$ は純粋状態であり，$\sum_{\boldsymbol{x}} P(\boldsymbol{x})\rho_{E,\boldsymbol{s}}(\boldsymbol{x}) = \sum_{\boldsymbol{t}} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|$ であるので，

$$\begin{aligned}
&I(P:\Lambda_E)\\
&=\sum_{\boldsymbol{s}} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})\Big(-\log(\mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})) + H\Big(\sum_{\boldsymbol{x}} P(\boldsymbol{x})\rho_{E,\boldsymbol{s}}(\boldsymbol{x})\Big)\\
&\qquad + \log(\mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})) - H(\rho_{E,\boldsymbol{s}}(\boldsymbol{x}))\Big)\\
&=\sum_{\boldsymbol{s}} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})H\Big(\sum_{\boldsymbol{x}} P(\boldsymbol{x})\rho_{E,\boldsymbol{s}}(\boldsymbol{x})\Big) = \sum_{\boldsymbol{s}} \mathrm{P}^{\mathbb{X}_1^r}(\boldsymbol{s})H(\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r=\boldsymbol{s}}) = H(\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r})
\end{aligned}$$

を得る．

P が一様分布でない場合は，分布 $P_{\boldsymbol{s}}(\boldsymbol{x}) := P(\boldsymbol{x}+\boldsymbol{s})$ についての平均を考えると，$\sum_{\boldsymbol{s}} \frac{1}{|\mathbb{X}^r|} P_{\boldsymbol{s}}$ は一様分布 P_{mix} となる．$I(P:\Lambda_E) = I(P_{\boldsymbol{s}}:\Lambda_E)$ であるから，(2.37) で与えた相互情報量の凹性より，およびエントロピーの凹性より，

$$I(P:\Lambda_E) \le I(P_{\mathrm{mix}}:\Lambda_E) = H(\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}) \le H(\mathrm{P}^{\mathbb{X}_2^r})$$

となり，題意を得る．　□

補題 5.6.2　(誤り確率による評価 [49])

$$d_1(P_{\mathrm{mix}}:\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E) \le 3\sqrt{1-\mathrm{P}^{\mathbb{X}_2^r}(0)}, \tag{5.57}$$

$$d_{1,\max}(P:\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E) \le 4\sqrt{1-\mathrm{P}^{\mathbb{X}_2^r}(0)}. \tag{5.58}$$

証明.　$\rho_{E,\boldsymbol{s}}(\boldsymbol{x})$ の対角成分からなる行列は $\sum_{\boldsymbol{t}} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|$ となることから $E_i = \sum_{\boldsymbol{s}} |(\boldsymbol{s},0)\rangle\langle(\boldsymbol{s},0)|$ となる場合に，(2.33) を適用することで以下を得る．

$$\left\| \sum_{\boldsymbol{t}} \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})| - \rho_{E,\boldsymbol{s}}(\boldsymbol{x}) \right\|_1 \le 3\sqrt{1-\mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(0|\boldsymbol{s})}. \tag{5.59}$$

$x \mapsto \sqrt{x}$ の凹性より，$P = P_{\mathrm{mix}}$ のとき，(5.57) を得る．

さらに，$E_i \rho_{E,\boldsymbol{s}}(\boldsymbol{x}) E_i = E_i \rho_{E,\boldsymbol{s}}(\boldsymbol{x}') E_i$ であるから，(2.32) を適用することで以下を得る．

$$
\begin{aligned}
&\|\rho_{E,\boldsymbol{s}}(\boldsymbol{x}) - \rho_{E,\boldsymbol{s}}(\boldsymbol{x}')\|_1 \\
&\le \|\rho_{E,\boldsymbol{s}}(\boldsymbol{x}) - E_i \rho_{E,\boldsymbol{s}}(\boldsymbol{x}) E_i\|_1 + \|E_i \rho_{E,\boldsymbol{s}}(\boldsymbol{x}') E_i - \rho_{E,\boldsymbol{s}}(\boldsymbol{x}')\|_1 \\
&\le 4\sqrt{1 - \mathrm{P}^{\mathbb{X}_2^r|\mathbb{X}_1^r}(0|\boldsymbol{s})}
\end{aligned}
$$

を得る．同様に $x \mapsto \sqrt{x}$ の凹性より，(5.58) を得る．　□

このように，Pauli 通信路については双対計算基底での誤り確率 $1 - P^{\mathbb{X}_2^r|\mathbb{X}_1^r}(0)$ を用いて，環境系への漏洩情報の量が評価できる．この事実は，一般の通信路にも拡張できる．

定理 5.6.3　一般の量子通信路 Λ について，その離散 Heisenberg 表現による twirling を $\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]$ とすると，以下が成り立つ．

$$
I(P_{\mathrm{mix}} : \Lambda_E) \le H(\mathrm{P}^{\mathbb{X}_2^r}) \le (1 - \mathrm{P}^{\mathbb{X}_2^r}(0)) \log |\mathbb{X}^r| + h(\mathrm{P}^{\mathbb{X}_2^r}(0)), \tag{5.60}
$$

$$
d_1(P_{\mathrm{mix}} : \Lambda_E) \le 3\sqrt{1 - \mathrm{P}^{\mathbb{X}_2^r}(0)}. \tag{5.61}
$$

上記のように，伝送したい情報が一様分布に従う場合，基準を $I(P_{\mathrm{mix}} : \Lambda_E)$ や $d_1(P_{\mathrm{mix}} : \Lambda_E)$ に限ると，一般の量子通信路でも Pauli 通信路と同様の評価が可能となる．しかし，基準を $d_{1,\max}(P_{\mathrm{mix}} : \Lambda_E)$ にとる場合には，一般の量子通信路について，Pauli 通信路と同様の評価が必ずしも可能とは限らない．

証明.　上記の不等式を示すために，以下の情報処理を考える．送信者が一様分布 P_{mix} に従って，秘密乱数 $\boldsymbol{x}$ を生成し，量子通信路 Λ を用いた以下のプロトコルで，情報を受信者に送ることを考える．$\boldsymbol{x}$ とは独立に一様分布 P_{mix} に従う乱数 $\boldsymbol{s}$ を生成し，量子通信路 Λ を通じて $|\boldsymbol{x} + \boldsymbol{s}\rangle$ を送る．このとき，盗聴者は古典情報 $|\boldsymbol{s}\rangle\langle\boldsymbol{s}|$ を獲得できるとする．そして，受信者側では受け取った状態に，$\mathsf{W}_{\mathbb{X}}(-\boldsymbol{s}, 0)$ を施す．したがって，受信者側の最終的な量子状態 $\mathsf{W}_{\mathbb{X}}(-\boldsymbol{s}, 0)\Lambda(|\boldsymbol{x} + \boldsymbol{s}\rangle\langle\boldsymbol{x} + \boldsymbol{s}|)\mathsf{W}_{\mathbb{X}}(\boldsymbol{s}, 0)$ となる．この操作を施したとき，秘密乱数 x と盗聴者が受け取る情報 $\Lambda_E(|\boldsymbol{x} + \boldsymbol{s}\rangle\langle\boldsymbol{x} + \boldsymbol{s}|) \otimes |\boldsymbol{s}\rangle\langle\boldsymbol{s}|$ との間の相互情報量は $\Lambda_E^{\boldsymbol{s}}(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|) := \Lambda_E(|\boldsymbol{x} + \boldsymbol{s}\rangle\langle\boldsymbol{x} + \boldsymbol{s}|)$ とすると，

$$\sum_{\boldsymbol{x}} \frac{1}{|\mathbb{X}^r|} D\left(\sum_{\boldsymbol{s}} \frac{1}{|\mathbb{X}^r|} \Lambda_E(|\boldsymbol{x}+\boldsymbol{s}\rangle\langle\boldsymbol{x}+\boldsymbol{s}|) \otimes |\boldsymbol{s}\rangle\langle\boldsymbol{s}| \right\| \left. \sum_{\boldsymbol{x}',\boldsymbol{s}'} \frac{1}{|\mathbb{X}^r|^2} \Lambda_E(|\boldsymbol{x}'+\boldsymbol{s}'\rangle\langle\boldsymbol{x}'+\boldsymbol{s}'|) \otimes |\boldsymbol{s}'\rangle\langle\boldsymbol{s}'| \right)$$

$$= \sum_{\boldsymbol{s}} \frac{1}{|\mathbb{X}^r|} I(P_{\mathrm{mix}} : \Lambda_E^{\boldsymbol{s}}) = I(P_{\mathrm{mix}} : \Lambda_E^{\boldsymbol{s}}) \tag{5.62}$$

となる．

次に，$|\boldsymbol{x}\rangle$ を入力とし，

$$\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}](|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)$$
$$= \sum_{\boldsymbol{s},\boldsymbol{t}} \frac{1}{|\mathbb{X}^r|^2} \mathsf{W}_{\mathbb{X}}(-\boldsymbol{s},-\boldsymbol{t}) \Lambda(\mathsf{W}_{\mathbb{X}}(\boldsymbol{s},\boldsymbol{t})|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\mathsf{W}_{\mathbb{X}}(-\boldsymbol{s},-\boldsymbol{t}))\mathsf{W}_{\mathbb{X}}(\boldsymbol{s},\boldsymbol{t})$$
$$= \sum_{\boldsymbol{s}} \frac{1}{|\mathbb{X}^r|} \mathsf{W}_{\mathbb{X}}(-\boldsymbol{s},0) \Lambda(|\boldsymbol{x}+\boldsymbol{s}\rangle\langle\boldsymbol{x}+\boldsymbol{s}|)\mathsf{W}_{\mathbb{X}}(\boldsymbol{s},0)$$

を出力とする量子通信を考える．このとき，上記の量子通信路の環境系は $\Lambda_E(|\boldsymbol{x}+\boldsymbol{s}\rangle\langle\boldsymbol{x}+\boldsymbol{s}|) \otimes |\boldsymbol{s}\rangle\langle\boldsymbol{s}|$ で記述される系よりも広い．したがって，相対エントロピーについての情報処理不等式より，

$$I(P_{\mathrm{mix}} : \Lambda_E^{\boldsymbol{s}})$$
$$= \sum_{\boldsymbol{x}} \frac{1}{|\mathbb{X}^r|} D\left(\sum_{\boldsymbol{s}} \frac{1}{|\mathbb{X}^r|} \Lambda_E(|\boldsymbol{x}+\boldsymbol{s}\rangle\langle\boldsymbol{x}+\boldsymbol{s}|) \otimes |\boldsymbol{s}\rangle\langle\boldsymbol{s}| \right\| \left. \sum_{\boldsymbol{x}',\boldsymbol{s}'} \frac{1}{|\mathbb{X}^r|^2} \Lambda_E(|\boldsymbol{x}'+\boldsymbol{s}'\rangle\langle\boldsymbol{x}'+\boldsymbol{s}'|) \otimes |\boldsymbol{s}'\rangle\langle\boldsymbol{s}'| \right)$$
$$\le \sum_{\boldsymbol{x}} \frac{1}{|\mathbb{X}^r|} D\left(\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|) \right\| \left. \sum_{\boldsymbol{x}'} \frac{1}{|\mathbb{X}^r|} D(\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E(|\boldsymbol{x}'\rangle\langle\boldsymbol{x}'|)\right)$$
$$= I(P_{\mathrm{mix}} : \Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E) \tag{5.63}$$

を得る．したがって，(5.55), (5.56) より，(5.60) を得る．

トレースノルムについても (5.62) と同様の式が成り立つため，同様にして，トレースノルムについての情報処理不等式と (5.57) を組み合わせることで

(5.61) を得る. □

5.6.2 秘匿性増強を行う場合

与えられた量子通信路 Λ について，計算基底と双対計算基底の誤り確率が非常に小さい場合には，漏洩情報と誤りの少ない通信が可能となる．しかし，これらの誤り確率が大きい場合，そのような通信路を用いると，そのままでは信頼性の高い通信は不可能である．5.3.2 項などで説明した量子誤り訂正を適用し，計算基底，双対計算基底の誤りを訂正すると，漏洩情報と誤りの少ない通信が可能となる．すなわち，量子誤り訂正を行って得られる量子通信路の双対計算基底の誤り確率を用いて，漏洩情報を評価できる．

量子通信路が Pauli 通信路 $\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]$ で与えられる場合，ねじれ条件を満たす C_2, C_1 からなる CSS 符号による量子誤り訂正を行い，$(x,y) \in \mathbb{X}^r/C_2^\perp \times \mathbb{X}^r/C_1^\perp = (C_1 \times C_2)^*$ の代表元 $(\boldsymbol{s}_x, \boldsymbol{t}_{x,y})$ に基づく復号化 D を考える．$([\boldsymbol{x}], [\boldsymbol{y}]) \in \mathbb{X}^r/C_2^\perp \times \mathbb{X}^r/C_1^\perp = (C_1 \times C_2)^*$ と $[\boldsymbol{s}] \in C_2^\perp/C_1$ に対して

$$\mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}([\boldsymbol{s}]) := \Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E(|[\boldsymbol{s}],[\boldsymbol{x}],[\boldsymbol{y}]\rangle\langle[\boldsymbol{s}],[\boldsymbol{x}],[\boldsymbol{y}]|)$$

$$\hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}([\boldsymbol{s}]) := (D \circ \Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}])_E(|[\boldsymbol{s}],[\boldsymbol{x}],[\boldsymbol{y}]\rangle\langle[\boldsymbol{s}],[\boldsymbol{x}],[\boldsymbol{y}]|)$$

とすると，空間 $\mathcal{H}_{[\boldsymbol{x}],[\boldsymbol{y}]}$ を用いた場合での盗聴者との間の相互情報量は $I(P, \mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]})$ で与えられる．量子通信路 $\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]$ の環境系は量子通信路 $D \circ \Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]$ の環境系の一部となる．したがって，すなわち，後者は前者の環境系に D の環境系 $\mathcal{E}_D$ を加えたものである．$\mathcal{E}_D$ について部分トレースに関する情報処理不等式より，

$$I(P, \mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le I(P, \hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \tag{5.64}$$

$$\le H(\mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J} + N\}^{C_1^\perp/C_2}) \tag{5.65}$$

$$\le (1 - \mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J} + N\}^{C_1^\perp/C_2}(0)) \log \dim \mathcal{H}_{[\boldsymbol{x}],[\boldsymbol{y}]}$$

$$+ h(\mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J} + N\}^{C_1^\perp/C_2}(0)) \tag{5.66}$$

を得る．ここで，(5.65) では $N = C_1 \times C_2$, $\mathcal{J} = \{(\boldsymbol{s}_x, \boldsymbol{t}_{x,y})\}_{(x,y)\in N^*}$ とおき，補題 5.6.1 を用いた．

また，上記と同様の情報処理不等式と補題5.6.2より，

$$d_1(P_{\mathrm{mix}}, \mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le d_1(P_{\mathrm{mix}}, \hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le 3\sqrt{1 - \mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J}+N\}^{C_1^{\perp}/C_2}(0)} \tag{5.67}$$

$$d_{1,\max}(P, \mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le d_{1,\max}(P, \hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le 4\sqrt{1 - \mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J}+N\}^{C_1^{\perp}/C_2}(0)} \tag{5.68}$$

を得る．したがって，$1 - \mathrm{P}^{\mathbb{X}^{2r}}\{\mathcal{J}+N\}^{C_1^{\perp}/C_2}(0)$ が十分小さくなるように，量子誤り訂正符号を選ぶと，秘匿性を保証した通信が可能となる．

量子誤り訂正を実行するには，量子的な操作が必要となり，コストがかかることが多い．以下に述べるように，量子通信路がPauli通信路 $\Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]$ で与えられる場合，5.1.5項で述べた $\mathbb{X}^r$ の符号化対 $C_1 \subset C_2^{\perp}$ を用いた秘匿性増強を伴った誤り訂正を行うと，上記のCSS符号による量子誤り訂正を行った場合と同等の秘匿性が保証できる[106]．$[\boldsymbol{x}] \in \mathbb{X}^r/C_2^{\perp}$ と $[\boldsymbol{s}] \in C_2^{\perp}/C_1$ に対して

$$\mathsf{W}_{\mathrm{mix},\boldsymbol{x}}(\boldsymbol{s}) := \sum_{\boldsymbol{s}' \in [\boldsymbol{s}]} \frac{1}{|C_1|} \Lambda[\mathsf{W}_{\mathbb{X}}^r, \mathrm{P}^{\mathbb{X}^{2r}}]_E(|\boldsymbol{s}'+\boldsymbol{y}\rangle\langle \boldsymbol{s}'+\boldsymbol{y}|)$$

とすると，

$$\sum_{[\boldsymbol{y}] \in \mathbb{X}^r/C_1^{\perp}} \frac{1}{|C_2|} \mathsf{W}_{[0],[\boldsymbol{y}]}([\boldsymbol{s}]) = \mathsf{W}_{\mathrm{mix},[0]}(\boldsymbol{s})$$

であるから，相対エントロピーとトレースノルムの接合凸性より，

$$I(P, \mathsf{W}_{\mathrm{mix},[0]}) \le \sum_{[\boldsymbol{y}] \in \mathbb{X}^r/C_1^{\perp}} \frac{1}{|C_2|} I(P, \mathsf{W}_{[0],[\boldsymbol{y}]})$$

$$d_1(P, \mathsf{W}_{\mathrm{mix},[0]}) \le \sum_{[\boldsymbol{y}] \in \mathbb{X}^r/C_1^{\perp}} \frac{1}{|C_2|} d_1(P, \mathsf{W}_{[0],[\boldsymbol{y}]})$$

$$d_{1,\max}(P, \mathsf{W}_{\mathrm{mix},[0]}) \le \sum_{[\boldsymbol{y}] \in \mathbb{X}^r/C_1^{\perp}} \frac{1}{|C_2|} d_{1,\max}(P, \mathsf{W}_{[0],[\boldsymbol{y}]})$$

を得る[46, 49]．したがって，(5.64), (5.66), (5.67), (5.68) より，それぞれの右辺は (5.66), (5.67), (5.68) の右辺で上から評価できる．

一般の量子通信路 Λ について，同様に，$\mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}([\boldsymbol{s}])$, $\hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}([\boldsymbol{s}])$, $\mathsf{W}_{\mathrm{mix},[\boldsymbol{x}]}(\boldsymbol{s})$ を定義すると，以下を得る．

$$\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_2|}I(P,\mathsf{W}_{\mathrm{mix},[\boldsymbol{x}]})$$
$$\le \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}I(P,\mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \tag{5.69}$$
$$\le \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}I(P,\hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \tag{5.70}$$
$$\le \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}H(P[D\circ\Lambda|_{\mathcal{H}_{([\boldsymbol{x}],[\boldsymbol{y}])}}]^{C_1^\perp/C_2}) \tag{5.71}$$
$$\le H(\sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}P[D\circ\Lambda|_{\mathcal{H}_{([\boldsymbol{x}],[\boldsymbol{y}])}}]^{C_1^\perp/C_2}) \tag{5.72}$$
$$= H(P[\Lambda]\{\mathcal{J}+N\}^{C_1^\perp/C_2}) \tag{5.73}$$
$$\le (1-P[\Lambda]\{\mathcal{J}+N\}^{C_1^\perp/C_2}(0))\log\dim\mathcal{H}_0 + h(P[\Lambda]\{\mathcal{J}+N\}^{C_1^\perp/C_2}(0)). \tag{5.74}$$

ここで，(5.69), (5.70), (5.71), (5.72), (5.73), (5.74) はそれぞれ，相対エントロピーの接合凸性，(5.64) と同様の情報処理不等式の適用，(5.60)，von Neumann エントロピーの凹性，(5.53), (2.40) から得られる．

同様に，$d_1(P,\mathsf{W}_{\mathrm{mix},[\boldsymbol{x}]})$ について以下が成り立つ．

$$\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_2|}d_1(P_{\mathrm{mix}},\mathsf{W}_{\mathrm{mix},[\boldsymbol{x}]})$$
$$\le \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}d_1(P_{\mathrm{mix}},\mathsf{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \tag{5.75}$$
$$\le \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}d_1(P_{\mathrm{mix}},\hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \tag{5.76}$$
$$\le \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{3}{|C_1||C_2|}\sqrt{1-P[D\circ\Lambda|_{\mathcal{H}_{([\boldsymbol{x}],[\boldsymbol{y}])}}]^{C_1^\perp/C_2}(0)} \tag{5.77}$$

$$\leq 3\sqrt{1 - \sum_{[\boldsymbol{y}]\in\mathbb{X}^r/C_1^\perp}\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_1||C_2|}P[D\circ\Lambda|_{\mathcal{H}_{([\boldsymbol{x}],[\boldsymbol{y}])}}]^{C_1^\perp/C_2}(0)} \quad (5.78)$$

$$= 3\sqrt{1 - P[\Lambda]\{\mathcal{J}+N\}^{C_1^\perp/C_2}(0)}. \quad (5.79)$$

ここで，(5.75), (5.76), (5.77), (5.78), (5.79) はそれぞれ，トレースノルム距離の接合凸性，(5.67) と同様の情報処理不等式の適用，(5.61)，$x \mapsto \sqrt{x}$ の凹性，(5.53) から得られる．

これらの議論をまとめると

$$\delta_{P[\Lambda]}[[C_1\times C_2]] := 1 - \max_{\mathcal{J}_{2,x}=\{\boldsymbol{t}_{x,y}\}}\sum_{[\boldsymbol{x}]\in\mathbb{X}_1^r/C_2^\perp}P[\Lambda]^{\mathbb{X}_1^r/C_2^\perp}([\boldsymbol{x}])P[\Lambda]^{\mathbb{X}_2^r|\mathbb{X}_1^r/C_2^\perp}(\mathcal{J}_{2,[\boldsymbol{x}]}+C_2|[\boldsymbol{x}]) \quad (5.80)$$

を用いた以下の定理を得る．

定理 5.6.4　$\mathbb{X}^r/C_2^\perp$ の一様分布に従って，ランダムに符号空間 $[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp$ を選び，部分群 $C_1 \subset C_2^\perp$ による秘匿性増強を用いた場合，一般の量子通信路 Λ による伝送を行うと，漏洩情報量は以下のように評価できる．

$$\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_2|}I(P,\mathsf{W}_{\mathrm{mix},[\boldsymbol{x}]}) \leq \delta[[C_1\times C_2]]\log\dim\mathcal{H}_0 + h(\delta[[C_1\times C_2]]), \quad (5.81)$$

$$\sum_{[\boldsymbol{x}]\in\mathbb{X}^r/C_2^\perp}\frac{1}{|C_2|}d_1(P_{\mathrm{mix}},\mathsf{W}_{\mathrm{mix},[\boldsymbol{x}]}) \leq 3\sqrt{\delta[[C_1\times C_2]]}. \quad (5.82)$$

なお，確率分布 $P[\Lambda]$ において，計算基底と双対計算基底での分布が独立であるとき，$\delta_{P[\Lambda]}[[C_1\times C_2]]$ は以下のように単純化できる．

$$\delta_{P[\Lambda]}[[C_1\times C_2]] = \delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2] = 1 - \max_{\mathcal{J}_2=\{\boldsymbol{t}_y\}}P[\Lambda]^{\mathbb{X}_2^r}(\mathcal{J}_2+C_2).$$

一般には，$\delta[[C_1\times C_2]] \leq \delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]$ となる．$P[\Lambda]^{\mathbb{X}_2^r}$ のみが既知であり，計算基底と双対計算基底との相関がわからないときには (5.81), (5.82) に $\delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]$ を代入した公式を使うことになる．

ここで，$(C_1 \times C_2)^*$ は $\mathbb{X}_2^r/C_2^\perp \times \mathbb{X}_2^r/C_1^\perp$ と同型であることに注意して，$(x, y) \in \mathbb{X}_2^r/C_2^\perp \times \mathbb{X}_2^r/C_1^\perp$ について，$\vec{s}_{x,y}$ を $(\boldsymbol{s}_x, \boldsymbol{t}_y)$ の形のものに限ると，(5.80) より

$$P[\Lambda]\{\{(\boldsymbol{s}_x, \boldsymbol{t}_y)\}_{(x,y)\in\mathbb{X}_2^r/C_2^\perp\times\mathbb{X}_2^r/C_1^\perp} + C_1 \times C_2\}_2(0)$$
$$= P[\Lambda]^{\mathbb{X}_2^r}(\{\boldsymbol{t}_y\}_{y\in\mathbb{X}_2^r/C_1^\perp} + C_2) \tag{5.83}$$

が成り立つ．したがって，不等式

$$\delta_{P[\Lambda]}[[C_1 \times C_2]] \leq 1 - \max_{\mathcal{J}_2=\{\boldsymbol{t}_y\}_{y\in\mathbb{X}_2^r/C_1^\perp}} P[\Lambda]^{\mathbb{X}_2^r}(\mathcal{J}_2 + C_2) = \delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2] \tag{5.84}$$

を得る．確率分布 $P[\Lambda]$ において，計算基底と双対計算基底での分布が独立であるときは，一般の $\vec{s}_{(x,y)}$ の形である $(\boldsymbol{s}_{x,y}, \boldsymbol{t}_{x,y})$ の形のものでも，

$$P[\Lambda]\{\{(\boldsymbol{s}_{x,y}, \boldsymbol{t}_{x,y})\}_{(x,y)\in\mathbb{X}_2^r/C_2^\perp\times\mathbb{X}_2^r/C_1^\perp} + C_1 \times C_2\}_2(0)$$
$$= \sum_{x\in\mathbb{X}_2^r/C_2^\perp} P[\Lambda]^{\mathbb{X}_1^r}(x)P[\Lambda]^{\mathbb{X}_2^r}(\{\boldsymbol{t}_{x,y}\}_{y\in\mathbb{X}_2^r/C_1^\perp} + C_2) \tag{5.85}$$

となるので，(5.84) において等号が成り立つ．

一方，$P[\Lambda]^{\mathbb{X}_2^r}$ のみが既知であり，計算基底と双対計算基底との相関があっても，それがわからないときは $\delta_{P[\Lambda]}[[C_1 \times C_2]]$ を評価することができない．しかし，(5.84) が成り立つことから，(5.81), (5.82) において，この値の代わりに $\delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]$ を代入した公式を使うことができる．

なお，安全性評価のためには，ここで紹介した方法の他に，Hash 関数のユニバーサル性を用いて評価する方法も知られている [100].

5.7 量子暗号（量子鍵配送）への応用

上記の議論から，位相エラーおよびビットエラーが既知である量子通信路が与えられれば，古典的な誤り訂正と秘匿性増強を適切に施せば秘匿通信が可能となる．しかし，位相エラーが一定のレベル以下であることを保証することは難しいことが多い．位相エラーを一定値以下であることを実質的に保証し，最

終的に安全な秘密乱数を遠隔地にある2者間で共有する方法が量子鍵配送である．その中でも最も基本的なプロトコルが1984年にBennett と Brassard によって提案されたプロトコル（**BB84 プロトコル**）[4] に，古典的な誤り訂正と秘匿性増強を加えたものである．一般には，量子暗号は量子鍵配送以外の量子系を用いた暗号プロトコル全般を指すが，本書では量子鍵配送以外の暗号プロトコルは扱わないので，量子暗号とは量子鍵配送を指すこととする．初めに誤り訂正と秘匿性増強を付加した離散 Heisenberg 表現 $\mathsf{W}_{\mathbb{X}}^r$ に基づく修正BB84プロトコルを述べる [87, 88, 106].

(1): 送信　Alice（送信者）は確率 $\frac{1}{2}$ でランダムに計算基底または双対計算基底を選び，その基底の下で $\mathbb{X}$ の要素である乱数をランダムに選んで量子通信路を用いて送る．この操作を複数回繰り返す．

(2): 受信　Bob（受信者）は確率 $\frac{1}{2}$ でランダムに計算基底または双対計算基底を選び，その基底に基づく測定を行い，$\mathbb{X}$ の要素である乱数を得る．この操作を複数回繰り返す．

(3): 基底照合　Alice と Bob は互いが選んだ基底についての情報を公開通信路上で交換し，基底が一致した部分に対応する乱数のみ残し，基底が一致しなかった部分に対応する乱数を捨てる．

(4): エラー確率推定　Alice は基底が一致した乱数のうちのそれぞれの基底の乱数について，割合 α の乱数を指定する．Alice と Bob はその乱数の値を公開通信路上で交換することで，残りの計算基底，双対計算基底の乱数についての両者の乱数の差が $s \in \mathbb{X}$ となる確率 $\mathrm{P}^{\mathbb{X}_1}(s)$, $\mathrm{P}^{\mathbb{X}_2}(s)$ を推定する．

(*)　以下，誤り訂正と秘匿性増強のプロトコルを行う．**(5)**, **(6)** は計算基底に関するものであるが，後に，双対計算基底についても同様のプロトコルを行う．

(5): 誤り訂正　上記のプロセスで得た r 桁の Alice の乱数列 $\boldsymbol{s}$ と Bob の乱数列 $\boldsymbol{s}'$ に対して，確率分布 $\mathrm{P}^{\mathbb{X}_1}$ で与えられるノイズを適切に誤り訂正できる $\mathbb{X}^r$ の部分群としての符号 $C_2^\perp$ を選ぶ．さらに，古典的な符号 $C_2^\perp$ の復号のための代表元の組 $\{\boldsymbol{s}^2_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{X}^r/C_2^\perp}$ を準備する．また，同時に別の代表元の組 $\{\boldsymbol{s}^1_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{X}^r/C_2^\perp}$ も合わせて準備する．

両者は r 桁の乱数に対して，$\mathbb{X}^r/C_2^\perp$ の情報 $[\boldsymbol{s}]$, $[\boldsymbol{s}']$ を公開通信路上で

交換する．Alice は C_2 の要素 $\boldsymbol{x} := \boldsymbol{s} - \boldsymbol{s}^1_{[\boldsymbol{s}]}$ を得る．Bob は C_2 の要素 $\boldsymbol{x}' := \boldsymbol{s}' - \boldsymbol{s}^1_{[\boldsymbol{s}]} - \boldsymbol{s}^2_{[\boldsymbol{s}'-\boldsymbol{s}]}$ を得る．

(6): 秘匿性増強 $C_2^\perp$ の部分群 C_1 を選ぶ．このとき，確率分布 $\mathrm{P}^{\mathbb{X}_2}$ にしたがう双対計算基底についての誤りが符号化対 $C_1^\perp/C_2$ によって適切に誤り訂正できるものを選ぶこととする．Alice と Bob は $C_2^\perp/C_1$ を最終的な秘密乱数とする．すなわち，Alice と Bob は乱数 $\boldsymbol{x}, \boldsymbol{x}' \in C_2^\perp$ を C_1 で割って得られる乱数を最終的な秘密乱数とする．

ここで，代表元の組 $\{\boldsymbol{s}^2_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{X}^r/C_2^\perp}$ は誤り訂正を行うためのものであるので，計算量を考慮しつつも，なるべく誤り確率が小さくなるように選ぶ．一方，別の代表元の組 $\{\boldsymbol{s}^1_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{X}^r/C_2^\perp}$ は $\boldsymbol{s} - \boldsymbol{s}^1_{[\boldsymbol{s}]}$ を $C_2^\perp$ の要素にすることだけが目的であるので，誤り確率はその選択に依存しない．したがって，単純に計算量を小さくするように選べばよい．そのため，C_2 の選択には，復号化に必要な代表元の組 $\{\boldsymbol{s}^2_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{X}^r/C_2^\perp}$ の計算量が少ないものを選ぶ配慮が必要である．また，C_1 については，復号の必要がないので，$C_1^\perp$ が C_2 を含む条件の下でランダムに選ぶことが可能となる．具体的には，$C_1^\perp$ を $C_2 \subset \mathbb{X}^r$ に対する $(1,\epsilon)$-二重ユニバーサル 2 となるように選ぶ [49, 111]．このときの安全性は，秘密乱数の生成元となる r 桁の乱数に対応する量子通信路を Λ とすると，定理 5.6.4 で与えられる量子通信を行ったときの安全性と同等である [106]．したがって，Λ から定義される確率分布 $P[\Lambda]$ を用いて，(5.81), (5.82) でその安全性が保証される．$P[\Lambda]$ を推定するためのプロセスが **(4): エラー確率推定**である．この方法では，計算基底でのエラーの確率分布と双対計算基底でのエラーの確率分布の相関が仮にあっても，それを推定することは不可能である．しかし，(5.84) により，$\delta_{P[\Lambda]}[[C_1 \times C_2]]$ を $\delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]$ に置き換えた場合の (5.81), (5.82) を用いて安全性が評価できる．

C_1 を上記の $(1,\epsilon)$-二重ユニバーサル 2 となるように選んだ場合の平均的な性能は以下のように評価できる．(5.81), (5.82) の右辺は $\delta_{P[\Lambda]}[[C_1 \times C_2]]$ について凹関数である．最終的な Alice の乱数が $\boldsymbol{x}$ であるときの盗聴者の持つ量子状態を $W^E(\boldsymbol{x})$ とし，最終的に Alice が得る乱数 $\boldsymbol{x}$ が従う確率分布を P とすると，(5.81) より，

$$\mathrm{E}_{C_1} I(P, W^E) \le \mathrm{E}_{C_1} \delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2] \log d + h(\mathrm{E}_{C_1} \delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]) \quad (5.86)$$

を得る．ここで，d は最終的な乱数サイズである．**(1): 送信**において，Alice が $\mathbb{X}$ の要素である乱数を一様分布に従って選んだ場合，最終的な Alice の乱数 $\boldsymbol{x}$ は一様分布 $P_{\max}$ に従う．このとき，(5.82) より，

$$\mathrm{E}_{C_1} d_1(P_{\max}, W^E) \le 3\sqrt{\mathrm{E}_{C_1} \delta_{P[\Lambda]^{\mathbb{X}_2^r}} [C_1^{\perp}/C_2]} \tag{5.87}$$

を得る．

一方，盗聴者にとって最適な場合に注目する基準 $\mathrm{E}_{C_1} d_{1,\max}(P_{\max}, W^E)$ についての評価は上記のプロトコルでは直接できない．このためには，若干のプロトコルの変更が必要である．すなわち，**(1): 送信**において，Alice の生成する乱数を一様分布に従って生成し，**(5): 誤り訂正**を以下のように修正する．このようにして得られるプロトコルを **twirling 型修正 BB84 プロトコル**とよぶ [46, 49].

(5)′: 誤り訂正　r 桁の乱数 $\boldsymbol{s}$(Alice), $\boldsymbol{s}'$(Bob) を元に，以下の方法で誤りのない乱数を共有する．Alice は新たな乱数 $\boldsymbol{x} \in C_2^{\perp}$ を生成し，$\boldsymbol{y} := \boldsymbol{x} - \boldsymbol{s}$ を公開通信路を通じて Bob に送る．Bob は $\boldsymbol{y} + \boldsymbol{s}' = \boldsymbol{x} - \boldsymbol{s} + \boldsymbol{s}'$ に対して，誤り訂正を施し，$\boldsymbol{x}' \in C_2^{\perp}$ を得る．

上記の r 桁の通信を表す量子通信路を Λ とする．上記の変形したプロトコルで乱数に $\boldsymbol{x} \in \mathbb{X}^r$ に関して盗聴者が獲得する情報は，以下のプロトコルにおいて，盗聴者が獲得する情報と同じである．この事実は計算基底の状態が $\mathsf{W}_{\mathbb{X}}^r(\boldsymbol{s}, 0)$ の作用に関して不変であることからわかる．

プロトコル A　Alice は $C_2^{\perp}$ 上の一様分布に従う乱数 $\boldsymbol{x} \in C_2^{\perp}$ と $\mathbb{X}^r$ 上の一様分布に従う乱数 $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{X}^r$ を生成し，$\boldsymbol{y}, \boldsymbol{z}$ を公開通信路を通じて Bob に送る．初期状態を $|\boldsymbol{x}\rangle$ とし，初期状態に $\mathsf{W}_{\mathbb{X}}^r(-\boldsymbol{y}, -\boldsymbol{z})$ を作用させる．その量子状態を量子通信路 Λ を通じて Bob に送る．Bob は受信した状態に $\mathsf{W}_{\mathbb{X}}^r(\boldsymbol{y}, \boldsymbol{z})$ を作用させ，その後に，計算基底で測定し，乱数 $\boldsymbol{x}''$ を得る．最後に Bob は乱数 $\boldsymbol{x}''$ に対して，誤り訂正を行う乱数 $\boldsymbol{x}' \in C_2^{\perp}$ を得る．

上記の**プロトコル A** では，乱数 $\boldsymbol{x} \in C_2^{\perp}$ を Λ に対して twirling を施した量子通信路 $\Lambda[\mathsf{W}_{\mathbb{X}}^r, P[\Lambda]]$ を用いて送っていることになる [30, 49]．Λ の環境系に加え送信前に $\mathsf{W}_{\mathbb{X}}^r(-\boldsymbol{y}, -\boldsymbol{z})$ を作用させる部分の環境系と受信後に $\mathsf{W}_{\mathbb{X}}^r(\boldsymbol{y}, \boldsymbol{z})$ を作用させる部分の環境系が盗聴者の支配下にあると仮定すると，盗聴者の

持つ情報は Pauli 量子通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, P[\Lambda]]$ の環境系の情報に一致する．したがって，twirling 型修正 BB84 プロトコルの安全性解析は**プロトコル A** の安全性解析に帰着できることから，Pauli 量子通信路 $\Lambda[\mathsf{W}^r_{\mathbb{X}}, P[\Lambda]]$ の場合の安全性解析に帰着でき，(5.58) が適用可能となる．(5.58) の右辺の凹性より以下を得る [49]．

$$\mathrm{E}_{C_1} d_{1,\max}(P_{\max}, W^E) \le 4\sqrt{\mathrm{E}_{C_1}\delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]}.$$

また，漸近的には真の分布 $P[\Lambda]^{\mathbb{X}_1^r}$, $P[\Lambda]^{\mathbb{X}_1^r}$ は **(4): エラー確率推定**で得られた分布 $\mathrm{P}^{\mathbb{X}_1}$, $\mathrm{P}^{\mathbb{X}_2}$ の r 次の独立同一分布に極めて近い．したがって，$\mathbb{X} = \mathbb{F}_q$ の場合には，$\mathrm{E}_{C_1}\delta_{P[\Lambda]^{\mathbb{X}_2^r}}[C_1^\perp/C_2]$ が 0 に収束するためには，5.3.4 項の議論より，漸近的には C_1 のサイズを $e^{rH(\mathrm{P}^{\mathbb{X}_2})}$ となるように選べば十分である．また，誤り訂正についても $C_2^\perp$ として理想的な符号を選べれば，C_2 のサイズが $e^{rH(\mathrm{P}^{\mathbb{X}_1})}$ となる範囲で誤り訂正が可能となる．したがって，漸近的生成レートが $\log q - H(\mathrm{P}^{\mathbb{X}_1}) - H(\mathrm{P}^{\mathbb{X}_2})$ となる安全な秘密乱数の生成が可能となる．

しかし，現実の系では r を無限にとることができず，有限の r での (5.86), (5.87) の右辺を評価する必要がある．このような議論は有限サイズの安全性とよばれる．この場合，真の分布 $P[\Lambda]^{\mathbb{X}_1^r}$, $P[\Lambda]^{\mathbb{X}_2^r}$ と **(4): エラー確率推定**で得られた分布 $\mathrm{P}^{\mathbb{X}_1}$, $\mathrm{P}^{\mathbb{X}_2}$ との関係を超幾何分布を用いて評価する必要があり，極めて煩雑な議論が必要となる [46, 53]．

第6章

ユニバーサルな情報処理

6.1　タイプ理論

本章では，Schur 双対を用いた様々なタイプのユニバーサルな情報処理を扱う．その準備として，以下では Schur 双対の漸近的振る舞いと密接な関係にある古典情報理論におけるタイプ理論を扱う．

以下では，確率空間 $\mathcal{X} := \{1, \ldots, k\}$ 上の確率分布はベクトル $\boldsymbol{p} = (p_1, \ldots, p_k)$ で記述され，その集合を $\mathcal{P}(k)$ または $\mathcal{P}(\mathcal{X})$ と記す．以下では，2.4 節で確率分布 $\boldsymbol{p}$ について定義したエントロピー $H(\boldsymbol{p}) = -\sum_{j=1}^{k} p_j \log p_j$ と異なる確率分布 $\boldsymbol{q} = (q_1, \ldots, q_k)$ との間で定義した相対エントロピー $D(\boldsymbol{p}\|\boldsymbol{q}) = \sum_{j=1}^{k} p_j(\log p_j - \log q_j)$ が重要な役割を果たす．そして，これらの分布の下で n 回の独立同一試行を行った場合を考える．このとき，確率空間は $\{1, \ldots, k\}^n$ で与えられ，その確率分布を $\boldsymbol{p}^n, \boldsymbol{q}^n$ と記す．加法性より，エントロピーと相対エントロピーは $H(\boldsymbol{p}^n) = nH(\boldsymbol{p})$, $D(\boldsymbol{p}^n\|\boldsymbol{q}^n) = nD(\boldsymbol{p}\|\boldsymbol{q})$ を満たす．このとき，個々のデータ $\vec{x} = (x_1, \ldots, x_n) \in \{1, \ldots, k\}^n$ に対して，そのタイプ $\boldsymbol{n} = (n_1, \ldots, n_k)$ を $n_j := \#\{l \,|\, x_l = j\}$ で定義する[1)]．つまり，このデータの経験分布は $\frac{\boldsymbol{n}}{n} = (\frac{n_1}{n}, \ldots, \frac{n_k}{n})$ で与えられる．なお，$\vec{x}$ のタイプを $\boldsymbol{n}(\vec{x})$ と記すことにする．このデータの出現確率は $\boldsymbol{n}(\vec{x}) = (n_1, \ldots, n_k)$ を用いて $\prod_{j=1}^{k} p_j^{n_j}$ と与えることができる．この値は，エントロピーと相対エン

---

1) Csiszár-Körner [21] では $\frac{\boldsymbol{n}}{n}$ をタイプして定義している．

トロピーを用いて以下のように表すことができる．

$$\prod_{j=1}^{k} p_j^{n_j} = e^{-n(D(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p}^n)+H(\frac{\boldsymbol{n}}{n}))}. \tag{6.1}$$

n 回の試行のタイプの集合を $\mathcal{T}_n^k$ または $\mathcal{T}_n(\mathcal{X})$ で表す．そして，タイプが $\boldsymbol{n} \in \mathcal{T}_n^k$ となるデータ $(\omega_1, \ldots, \omega_n) \in \{x_1, \ldots, x_k\}^n$ の集合を $T_{\boldsymbol{n}}$ とする．するとその個数 $|T_{\boldsymbol{n}}|$ は $C(\boldsymbol{n}) := \frac{n!}{n_1!n_2!\ldots n_k!}$ に一致する．

したがって，n 次の k 項分布は $\mathcal{T}_n^k$ 上の確率分布 $\mathrm{Mul}[\boldsymbol{p}, n]$ として，

$$\mathrm{Mul}[\boldsymbol{p}, n](\boldsymbol{n}) := C(\boldsymbol{n}) \prod_{j=1}^{k} p_j^{n_j}, \quad \boldsymbol{n} = (n_1, \ldots, n_k) \in \mathcal{T}_n^k \tag{6.2}$$

で与えられる．そして，$|\mathcal{T}_n^k|$ はそれぞれの n_j は $0, \ldots, n$ のどれかをとり，k 番目の n_k は他の値から自動的に決まるので，$|\mathcal{T}_n^k| \le (n+1)^{k-1}$ を得る．**Stirling の公式** $n! \cong \sqrt{2\pi n} n^n e^{-n}$ を用いると，

$$\begin{aligned}
\log|\mathcal{T}_n^k| &= \log \binom{n+k}{k-1} + o(1) \\
&= \log \frac{\sqrt{2\pi(n+k)}(n+k)^{n+k} e^{-(n+k)}}{\sqrt{2\pi(n+1)}(n+1)^{n+1} e^{-(n+1)} (k-1)!} + o(1) \\
&= \log \frac{(n+k)^{k-1}}{(k-1)!} \sqrt{\frac{n+k}{n+1}} e^{-k+1} (1 + \frac{k-1}{n+1})^{n+1} + o(1) \\
&= \log \frac{(n+k)^{k-1}}{(k-1)!} + o(1) \\
&= (k-1)\log n - \log(k-1)! + o(1)
\end{aligned} \tag{6.3}$$

となる．

さらに，$C(\boldsymbol{n})$ は以下のように評価できる．

$$\frac{1}{(n+1)^{k-1}} e^{nH(\frac{\boldsymbol{n}}{n})} \le C(\boldsymbol{n}) \le e^{nH(\frac{\boldsymbol{n}}{n})}. \tag{6.4}$$

したがって，(6.1), (6.4) より，

$$\frac{1}{(n+1)^{k-1}} e^{-nD(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p})} \le \boldsymbol{p}^n(T_{\boldsymbol{n}}) \le e^{-nD(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p})} \tag{6.5}$$

を得る．

上記の議論から確率変数 $\frac{\boldsymbol{n}}{n}$ は $\boldsymbol{p}$ に確率収束することがわかる．すなわち，$\boldsymbol{p}$ を含まない集合 $\mathcal{R}$ に $\frac{\boldsymbol{n}}{n}$ が含まれる確率は n に関して指数的に 0 に収束する．そのため，$\boldsymbol{p}$ が未知であるとき，$\frac{\boldsymbol{n}}{n}$ を $\boldsymbol{p}$ の推定値として用いることができる．$\frac{\boldsymbol{n}}{n}$ を推定値として用いる場合，その精度を表すのが，確率 $\Pr\{\frac{\boldsymbol{n}}{n} \in \mathcal{R}\}$ の減少指数である．この種の指数に関する評価のことを**大偏差型評価**とよぶ．これまでの議論を整理すると，以下の大偏差型評価に関する補題を得る．

補題 6.1.1 経験分布 $\frac{\boldsymbol{n}}{n}$ が $\mathcal{P}(k)$ の部分集合 $\mathcal{R}$ に含まれる確率は $\mathcal{R}_{\boldsymbol{n}} := \{\boldsymbol{q} \in \mathcal{R} \,|\, n\boldsymbol{q} \in \mathcal{T}_n^k\}$ を用いると，以下のように評価できる．

$$\frac{1}{(n+1)^{k-1}} \max_{\boldsymbol{q} \in \mathcal{R}_n} e^{-nD(\boldsymbol{q}\|\boldsymbol{p})} \le \sum_{\frac{\boldsymbol{n}}{n} \in \mathcal{R}} \boldsymbol{p}^n(T_{\boldsymbol{n}}) \le (n+1)^{k-1} \max_{\boldsymbol{q} \in \mathcal{R}} e^{-nD(\boldsymbol{q}\|\boldsymbol{p})}. \tag{6.6}$$

この事実から，以下を得る．

$$\lim_{n\to\infty} \frac{-1}{n} \log \sum_{\frac{\boldsymbol{n}}{n} \in \mathcal{R}} \boldsymbol{p}^n(T_{\boldsymbol{n}}) = \min_{\boldsymbol{q} \in \mathcal{R}} D(\boldsymbol{q}\|\boldsymbol{p}). \tag{6.7}$$

したがって，$\mathcal{R}$ に $\{\boldsymbol{p} \in \mathcal{P}(k) \,|\, H(\boldsymbol{p}) \le R\}$, $\{\boldsymbol{p} \in \mathcal{P}(k) \,|\, H(\boldsymbol{p}) \ge R\}$ などを代入すると，以下の補題を得る．

補題 6.1.2

$$\lim_{n\to\infty} \frac{-1}{n} \log \sum_{\boldsymbol{n}: H(\frac{\boldsymbol{n}}{n}) \le R} \boldsymbol{p}^n(T_{\boldsymbol{n}}) = \min_{\boldsymbol{q}: H(\boldsymbol{q}) \le R} D(\boldsymbol{q}\|\boldsymbol{p}), \tag{6.8}$$

$$\lim_{n\to\infty} \frac{-1}{n} \log \sum_{\boldsymbol{n}: H(\frac{\boldsymbol{n}}{n}) \ge R} \boldsymbol{p}^n(T_{\boldsymbol{n}}) = \min_{\boldsymbol{q}: H(\boldsymbol{q}) \ge R} D(\boldsymbol{q}\|\boldsymbol{p}). \tag{6.9}$$

なお，右辺の量については (2.70), (2.71) により，$\psi(s|\boldsymbol{p})$ を用いて表すことができる．

さらに，以下の補題が知られている [20].

補題 6.1.3　$\boldsymbol{n}$ が多項分布 $\mathrm{Mul}[\boldsymbol{p}, n]$ に従う確率変数であるとき，確率変数 $\frac{\boldsymbol{n}}{n}$ は $\boldsymbol{p}$ に確率収束する．さらに，確率変数 $\frac{\boldsymbol{n}-n\boldsymbol{p}}{\sqrt{n}}$ の極限分布は共分散行列が

$$C_{i,j} = \begin{cases} -p_i p_j & i \neq j \text{ のとき} \\ p_i(1-p_i) & i = j \text{ のとき} \end{cases}$$

となる正規分布となる．

これら2つの補題 6.1.1, 6.1.3 を量子系を適用しよう．これらの補題は密度行列を固有ベクトルがわかっているときに，固有値 $\boldsymbol{p}$ を推定したときに誤差の評価を大偏差型および極限分布のそれぞれの基準で与えていることになる．例えば，固有ベクトルが計算基底であるときは状態族 $\{\rho(\boldsymbol{p})\}$ の状態推定となる．

補題 6.1.4　$\boldsymbol{n} \in \mathcal{T}_n^k$ が多項分布 $\mathrm{Mul}[\boldsymbol{p}, n]$ に従うとする．$\boldsymbol{n}$ の期待値は以下を満たす．

$$\lim_{n\to\infty} \mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n]} \log \frac{n!}{\boldsymbol{n}!} - nH(\boldsymbol{p}) + \frac{k-1}{2}\log n$$
$$= -\frac{k-1}{2}\log 2\pi e - \frac{1}{2}\sum_{j=1}^{k}\log p_j. \tag{6.10}$$

証明.　Stirling の公式より，$n! \cong \sqrt{2\pi n} n^n e^{-n}$ となるので，

$$\log\frac{n!}{\boldsymbol{n}!} = nH\left(\frac{\boldsymbol{n}}{n}\right) - \frac{k-1}{2}\log n - \frac{k-1}{2}\log 2\pi - \frac{1}{2}\sum_{j=1}^{k}\log\frac{n_j}{n} + o(1)$$

を得る．さらに，$\frac{n_j}{n}$ が p_j の近傍にあるとき，$H(\frac{\boldsymbol{n}}{n})$ について2階の微分まで考慮して Taylor 展開を行うと，

$$nH\left(\frac{\boldsymbol{n}}{n}\right) = nH(\boldsymbol{p}) + \sum_{j=1}^{k}\frac{\partial H(\boldsymbol{p})}{\partial p_j}(n_j - p_j) + \frac{1}{2}\left(n - \sum_{j=1}^{k}\frac{n_j^2}{p_j n}\right) + o(1)$$

を得る．n_j^2 の期待値は $np_j(1-p_j) + (np_j)^2$ であるから，$\frac{1}{2}\mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n]}(n - \sum_{j=1}^{k}\frac{n_j^2}{p_j n}) = \frac{k-1}{2}$ で与えられる．したがって，$\frac{n_j}{n}$ が p_j に確率収束すること

から，

$$
\begin{aligned}
&\mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n]} \log \frac{n!}{\boldsymbol{n}!} \\
&= nH(\boldsymbol{p}) + \sum_{j=1}^{k} \frac{\partial H(\boldsymbol{p})}{\partial p_j} \mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n]}(n_j - p_j) + \frac{1}{2}\mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n]}\left(n - \sum_{j=1}^{k} \frac{n_j^2}{p_j n}\right) \\
&\quad - \frac{k-1}{2}\log n - \frac{k-1}{2}\log 2\pi - \mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n]}\frac{1}{2}\sum_{j=1}^{k}\log\frac{n_j}{n} + o(1) \\
&= nH(\boldsymbol{p}) + \frac{k-1}{2} - \frac{k-1}{2}\log n - \frac{k-1}{2}\log 2\pi - \frac{1}{2}\sum_{j=1}^{k}\log p_j + o(1)
\end{aligned}
$$

となり，題意を得る． □

6.2 Schur 双対の漸近理論

6.2.1 Schur 双対の漸近的取り扱い

次に，Schur 双対に現れる量の漸近的挙動を扱う．Schur 双対については [37] の (4.44) で与えられているが，単純化のため，$\boldsymbol{n} \in \mathcal{Y}_n^r$ が与えられたときの SU(r) の既約な表現空間 $\mathcal{U}_{in^*(\boldsymbol{n})}(\mathrm{SU}(r))$，$S_n$ の既約な表現空間 $\mathcal{U}_{\boldsymbol{n}}(S_n)$ をそれぞれ，$\mathcal{U}_{\boldsymbol{n}}, \mathcal{V}_{\boldsymbol{n}}$ と略記する．したがって，Schur 双対は以下のように単純化される．

$$
(\mathbb{C}^r)^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^r} \mathcal{W}_{\boldsymbol{n}}, \quad \mathcal{W}_{\boldsymbol{n}} := \mathcal{U}_{\boldsymbol{n}} \otimes \mathcal{V}_{\boldsymbol{n}}. \tag{6.11}
$$

そして，$\mathcal{W}_{\boldsymbol{n}}$ への射影を $P_{\boldsymbol{n}}$ と記す．以下，$\mathbb{C}^r$ 上の密度行列 ρ の対角成分が $p_1 \ge \cdots \ge p_r$ を満たす確率分布 $\boldsymbol{p} = (p_1, \ldots, p_r)$ で与えられている場合について考える．このような確率分布の集合を $\mathcal{Y}(r)$ と記す．このときの次元 $\dim \mathcal{U}_{\boldsymbol{n}}$ は [37] の (4.35) によって与えられるが，各 $j < l$ について，$\frac{l-j+n_l-n_j}{l-j} \le n_l - n_j + 1 \le n+1$ となることに注意すると，

$$
\dim \mathcal{U}_{\boldsymbol{n}} = \prod_{1 \le j < l \le r} \frac{l-j+n_l-n_j}{l-j} \le (n+1)^{r(r-1)/2} \tag{6.12}
$$

と評価でき，

$$\log \dim \mathcal{U}_{\boldsymbol{n}} = \frac{r(r-1)}{2}\log n + \sum_{1\le j<l\le r}\log\left(\frac{n_l}{n}-\frac{n_j}{n}\right) - \sum_{j=1}^{r-1}(r-j)\log j + o(1) \tag{6.13}$$

となる．

そして，$\mathcal{Y}_n^r$ の要素の数 $|\mathcal{Y}_n^r|$ （深さが r 以下であり，大きさ n の Young diagram の数）は以下のように評価できる．

$$|\mathcal{Y}_n^r| \le |\mathcal{T}_n^r| \le (n+1)^{r-1}. \tag{6.14}$$

$\mathcal{T}_n^r$ の要素 $\boldsymbol{n}$ でその成分に同じ値を持つものが存在するものの割合は $n\to\infty$ の極限で 0 に収束する．したがって，$n\to\infty$ の極限では，$\mathcal{Y}_n^r$ の要素の数は $\mathcal{T}_n^r$ の要素の数の $\frac{1}{r!}$ であると考えることができる．(6.3) より，以下を得る．

$$\log|\mathcal{Y}_n^r| \cong (r-1)\log n - \log(r-1)!r! + o(1). \tag{6.15}$$

さらに，[37] の (2.58) より，$r\ge j>i\ge 1$ について，$n_i+j \ge (n_i-n_j-i+j)$ であることに注意すると，次元 $\dim\mathcal{V}_{\boldsymbol{n}}$ は以下のように評価できる．

$$\begin{aligned}\dim\mathcal{V}_{\boldsymbol{n}} &= \frac{n!}{(n_1+r-1)!(n_2+r-2)!\dots r_d!}\prod_{j>i}(n_i-n_j-i+j)\\ &= \frac{n!}{n_1!n_2!\dots n_r!}\prod_{j>i}\frac{n_i-n_j-i+j}{n_i+j-1} \le C(\boldsymbol{n}) \le e^{nH(\frac{\boldsymbol{n}}{n})}.\end{aligned} \tag{6.16}$$

$r\ge j>i\ge 1$ について，$(n_i-n_j-i+j)\ge 1$ であるから，(6.4) を用いると逆方向の評価は以下のようにできる．

$$\begin{aligned}\dim\mathcal{V}_{\boldsymbol{n}} &\ge \frac{n!}{(n_1+r-1)!(n_2+r-2)!\cdots n_d!}\\ &\ge \frac{n!}{n_1!n_2!\cdots n_d!}\left(\frac{1}{n+r}\right)^{r-1}\left(\frac{1}{n+r}\right)^{r-2}\cdots\left(\frac{1}{n+r}\right)^{0}\\ &= C(\boldsymbol{n})\left(\frac{1}{n+r}\right)^{\frac{r(r-1)}{2}} \ge e^{nH(\frac{\boldsymbol{n}}{n})}(n+r)^{-\frac{(r+2)(r-1)}{2}}.\end{aligned} \tag{6.17}$$

6.2.2 ユニバーサルな固有値の推定

6.1 節で扱った多項分布の推定の議論を量子系に適用すると，基底がわかっている密度行列の固有値を推定することが可能となる．しかし，量子系では一般には密度行列の基底がわかっていないことが多い．このような場合に，密度行列の固有値を推定するには，基底の情報なしに固有値を推定することが求められる．以下では，n 階テンソル積空間 $\mathcal{H}^{\otimes n}$ に未知の密度行列 ρ の n 階のテンソル積状態 $\rho^{\otimes n}$ が準備されたとき，$\mathcal{H}^{\otimes n}$ 上の測定を用いて ρ の固有値を推定する問題を扱う．

このとき，密度行列は固有値の列 $\boldsymbol{p}$ と $\mathrm{SU}(r)$ を $\rho(\boldsymbol{p})$ の固定化群 H で割った等質空間の要素 $[g] \in \mathrm{SU}(r)/H$ を用いて $g\rho(\boldsymbol{p})g^\dagger$ と記述される．推定値は $\hat{\boldsymbol{p}}$ となり，誤差は $\hat{\boldsymbol{p}}$ と $\boldsymbol{p}$ の関数として与えられる．この設定は，注意 4.1.3 で述べた一般的な群共変性を持つモデルである．すなわち，状態を記述するパラメータ空間 Θ が $\mathbb{C}^r$ 上の密度行列全体であり，推定値の集合が $\mathcal{Y}(r)$ となる．また，群の作用の下で $\hat{\boldsymbol{p}}$ と $\boldsymbol{p}$ は不変であるので，誤差を与える関数も群不変性を満たす．したがって，定理 4.1.1 の一般化が成り立ち，最適な測定を，(4.8) を満たす測定，すなわち

$$g^{\otimes n} M_{\hat{\boldsymbol{p}}} g^{\otimes n \dagger} = M_{\hat{\boldsymbol{p}}} \tag{6.18}$$

を満たす測定に限ることができる．このとき，POVM 要素 $M_{\hat{\boldsymbol{p}}}$ は既約空間上の射影の定数倍となる．

以下では，$\frac{\boldsymbol{n}}{n}$ にのみ値を持つ POVM $M_{\frac{\boldsymbol{n}}{n}} := P_{\boldsymbol{n}}$ で推定することにする [81, 43, 85]．この POVM は条件 (6.18) を満たす．この推定値の振る舞いを調べるために，確率分布 $Q[\rho^{\otimes n}](\boldsymbol{n}) := \mathrm{Tr}\, P_{\boldsymbol{n}} \rho^{\otimes n}$ に注目する．特に，ρ の固有値が $\boldsymbol{p}$ で与えられる場合は確率分布 $Q[\rho^{\otimes n}(\boldsymbol{p})]$ を $Q_{\boldsymbol{p}}$ と記す．

ρ の値域が $\mathcal{H} = \mathbb{C}^r$ 全体のとき，ρ は $\mathrm{GL}(r)$ の要素と見なすことができる．したがって，$\rho^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^r} \mathsf{f}_{\boldsymbol{n}}(\rho) \otimes I_{\mathcal{V}_{\boldsymbol{n}}}$ となる．

一方，ρ の値域が $\mathcal{H} = \mathbb{C}^r$ の部分空間 $\mathcal{K} = \mathbb{C}^{r'}$ で与えられるときは，やや話が複雑である．$\mathcal{K}^{\otimes n}$ の直和分解を $\mathcal{K}^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} \mathcal{U}'_{\boldsymbol{n}} \otimes \mathcal{V}_{\boldsymbol{n}}$ で与える．このとき，$\mathsf{f}_{\boldsymbol{n}}(\rho)$ は $\mathcal{U}'_{\boldsymbol{n}}$ 上の行列となる．$\mathcal{U}'_{\boldsymbol{n}}$ は $\mathcal{U}_{\boldsymbol{n}}$ の部分空間であるので，$\mathsf{f}_{\boldsymbol{n}}(\rho)$ を $\mathcal{U}_{\boldsymbol{n}}$ 上の行列と見なすことができる．すると，$\rho^{\otimes n}$ は $\rho^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} \mathsf{f}_{\boldsymbol{n}}(\rho) \otimes I_{\mathcal{V}_{\boldsymbol{n}}}$ と書ける．したがって，$\mathcal{W}'_{\boldsymbol{n}} := \mathcal{U}'_{\boldsymbol{n}} \otimes \mathcal{V}_{\boldsymbol{n}}$ への射

影を $P'_{\boldsymbol{n}}$ とすると，$\operatorname{Tr}\rho^{\otimes n}P_{\boldsymbol{n}} = \operatorname{Tr}\rho^{\otimes n}P'_{\boldsymbol{n}}$ を得る．この式は ρ の値域よりも広い空間を考えても，測定値の振る舞いは ρ の値域についてのテンソル積空間の既約分解に基づく測定と同じ測定値の分布が得られることを示している．さらに，上記の議論から $\|P_{\boldsymbol{n}}\rho^{\otimes n}P_{\boldsymbol{n}}\| = \prod_{i=1}^r p_i^{n_i}$ を得る．

以下，$Q[\rho^{\otimes n}](\boldsymbol{n})$ の振る舞いを調べる．$P_{\boldsymbol{n}}\rho^{\otimes n}P_{\boldsymbol{n}}$ のノルムは $\prod_{i=1}^r p_i^{n_i}$ となることに注意する．すると，(6.1), (6.12), (6.16) より，

$$\begin{aligned}\operatorname{Tr} P_{\boldsymbol{n}}\rho^{\otimes n} &\le \dim \mathcal{V}_{\boldsymbol{n}} \cdot \dim \mathcal{U}_{\boldsymbol{n}} \cdot \prod_{i=1}^r p_i^{n_i} \\ &\le e^{nH\left(\frac{\boldsymbol{n}}{n}\right)}(n+1)^{r(r-1)/2} e^{-n(D(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p}^n)+H(\frac{\boldsymbol{n}}{n}))} \\ &= (n+1)^{r(r-1)/2} e^{-nD(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p}^n)} \end{aligned} \tag{6.19}$$

を得る．逆に，$\rho^{\otimes n}$ を $\mathrm{GL}(r,\mathbb{C})$ の表現とみた場合，これが働くのは空間 $\mathcal{U}_{\boldsymbol{n}}$ のみであり，$\mathcal{V}_{\boldsymbol{n}}$ は重複度を表す空間であるので，(6.17) より，

$$\begin{aligned}\operatorname{Tr} P_{\boldsymbol{n}}\rho^{\otimes n} &\ge \dim \mathcal{V}_{\boldsymbol{n}} \cdot \prod_{i=1}^r p_i^{n_i} \\ &\ge e^{nH\left(\frac{\boldsymbol{n}}{n}\right)}(n+r)^{-\frac{(r+2)(r-1)}{2}} e^{-n(D(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p}^n)+H(\frac{\boldsymbol{n}}{n}))} \\ &= (n+r)^{-\frac{(r+2)(r-1)}{2}} e^{-nD(\frac{\boldsymbol{n}}{n}\|\boldsymbol{p}^n)} \end{aligned}$$

となる．したがって，補題6.1.1と同様に，以下の補題を得る．

補題 6.2.1　状態が $\rho^{\otimes n}$ であるときに，測定 $\{P_{\boldsymbol{n}}\}_{\boldsymbol{n}\in\mathcal{Y}_n^r}$ を行ったとする．このとき，$\frac{\boldsymbol{n}}{n}$ が $\mathcal{Y}(r)$ の部分集合 $\mathcal{R}$ に含まれる確率は $\mathcal{R}_n := \{\boldsymbol{q}\in\mathcal{Y}\,|\,n\boldsymbol{q}\in\mathcal{Y}_n^r\}$ を用いると，以下のように評価できる．

$$\begin{aligned}(n+r)^{-\frac{(r+2)(r-1)}{2}} \max_{\boldsymbol{q}\in\mathcal{R}_n} e^{-nD(\boldsymbol{q}\|\boldsymbol{p})} &\le \sum_{\frac{\boldsymbol{n}}{n}\in\mathcal{R}} \operatorname{Tr} P_{\boldsymbol{n}}\rho^{\otimes n} \\ &\le (n+1)^{\frac{(r+2)(r-1)}{2}} \max_{\boldsymbol{q}\in\mathcal{R}} e^{-nD(\boldsymbol{q}\|\boldsymbol{p})}. \end{aligned} \tag{6.20}$$

補題6.1.1と補題6.2.1を比較すると，一定以上外れた推定値についての同じ減少指数を得る．すなわち，基底の情報がない場合でも，基底の情報がある場合と同じ，外れた推定値について減少指数となる．

さらに，補題6.2.1より，$\boldsymbol{n}$ が確率分布 $Q[\rho^{\otimes n}]$ に従う確率変数であるとき，確率変数 $\frac{\boldsymbol{n}}{n}$ は $\boldsymbol{p}$ に確率収束する．より緻密な評価として，以下の補題が成り立つ [85].

補題 6.2.2 $p_1 > \cdots > p_r$ とする．$\boldsymbol{n}$ が確率分布 $Q[\rho^{\otimes n}]$ に従う確率変数であるとき，確率変数 $\frac{\boldsymbol{n}-n\boldsymbol{p}}{n}$ の期待値は0 に収束し，そのオーダーは $O(\frac{1}{n})$ である．さらに，確率変数 $\frac{\boldsymbol{n}-n\boldsymbol{p}}{\sqrt{n}}$ の極限分布は共分散行列が

$$C_{i,j} = \begin{cases} -p_i p_j & i \neq j \text{ のとき} \\ p_i(1-p_i) & i = j \text{ のとき} \end{cases}$$

となる正規分布となる．このため，ϵ_n が $\sqrt{n}\epsilon_n \to \infty$ を満たすとき，$|\frac{\boldsymbol{n}}{n} - \boldsymbol{p}| \leq \epsilon_n$ となる確率は 1 に収束する．

補題6.1.3と補題6.2.2を比較すると，推定値が真の値に近い場合，同じ極限分布を得る．推定値が真の値に近い場合での，漸近的振る舞いについても，基底の情報の有無で差が生じないことがわかる．このように，固有値の推定は基底に依存せず，ユニバーサルに行うことができる．

証明. (4.42) より，

$$\chi_{\boldsymbol{n}}(\rho) = \frac{\sum_{\sigma' \in S_r} \mathrm{sgn}(\sigma') \prod_{l=1}^r a_l^{n_{\sigma'(l)} + \delta_{\sigma'(l)}}}{\prod_{j<l}(a_l - a_j)}$$

となる．補題6.2.1より，$\boldsymbol{n}$ が $n\boldsymbol{p}$ に十分近い場合以外の確率はほぼ0 である．すなわち，$\epsilon > 0$ に対して，$\frac{n_j}{n} \in (p_j - \epsilon, p_j + \epsilon)$ となる場合のみ考える．ここで，$p_{j-1} - \epsilon > p_j + 2\epsilon$ となるように，$\epsilon > 0$ を選ぶとする．ここで，簡単のため，σ' を 1 と 2 の互換とする．このとき，

$$\frac{\prod_{l=1}^r a_l^{n_{\sigma'(l)} + \delta_{\sigma'(l)}}}{\prod_{l=1}^r a_l^{n_l + \delta_l}} \leq \frac{\prod_{l=1}^r a_l^{\delta_{\sigma'(l)}}}{\prod_{l=1}^r a_l^{\delta_l}} \left(\frac{a_2}{a_1}\right)^{2n\epsilon}$$

は指数的に 0 に収束する．同じようにして，任意の単位元でない $\sigma' \in S_r$ についても，上記の値は 0 に収束する．したがって，σ' が単位元以外の場合の項は無視できる．

[37] の (2.57) より，$\boldsymbol{n}^\sigma := \boldsymbol{n} + \boldsymbol{\delta} - \sigma(\boldsymbol{\delta})$ とすると，上記の条件から，このベクトルの要素は全て正である．したがって，

$$
\begin{aligned}
Q[\rho^{\otimes n}](\boldsymbol{n}) &= \chi_{\boldsymbol{n}}(\rho) \cdot \dim \mathcal{V}_{\boldsymbol{n}} \\
&\cong \frac{\prod_{l=1}^r a_l^{n_l+\delta_l}}{\prod_{j<l}(a_l - a_j)} \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \frac{n!}{[\boldsymbol{n} + \boldsymbol{\delta} - \sigma(\boldsymbol{\delta})]!} \\
&= \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \frac{\prod_{l=1}^r a_l^{\delta_{\sigma(l)}}}{\prod_{j<l}(a_l - a_j)} \prod_{l=1}^r a_l^{n_l^\sigma} \frac{n!}{\boldsymbol{n}^\sigma!}
\end{aligned}
$$

を得る．右辺は，$\sigma \in S_r$ に応じて決まる確率分布 $\mathrm{Mul}[\boldsymbol{p}, n, \sigma](\boldsymbol{n}) := \prod_{l=1}^r a_l^{n_l^\sigma} \cdot \frac{n!}{\boldsymbol{n}^\sigma!}$ を係数 $\mathrm{sgn}(\sigma) \frac{\prod_{l=1}^r a_l^{\delta_{\sigma(l)}}}{\prod_{j<l}(a_l - a_j)}$ で足し合わせたものと見なすことができる．確率分布 $\mathrm{Mul}[\boldsymbol{p}, n, \sigma](\boldsymbol{n})$ の下での $\frac{\boldsymbol{n}}{n}$ の期待値は $\boldsymbol{p} + \frac{\sigma(\boldsymbol{\delta}) - \boldsymbol{\delta}}{n}$ となる．したがって，$\frac{\boldsymbol{n}}{n} - \boldsymbol{p}$ は 0 に確率収束し，その期待値はオーダー $O(\frac{1}{n})$ で 0 に収束する．さらに，上記の議論から $\frac{\boldsymbol{n}^\sigma}{\sqrt{n}} - \frac{\boldsymbol{n}}{\sqrt{n}}$ は 0 に確率収束するので，$\boldsymbol{n}$ が上記のどの確率分布に従う場合でも，その極限分布は共分散行列が $C_{i,j}$ となる正規分布となる．

さらに，Vandermonde（ファンデルモンド）の行列式より，

$$
\sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \frac{\prod_{l=1}^r a_l^{\delta_{\sigma(l)}}}{\prod_{j<l}(a_l - a_j)} = 1 \tag{6.21}
$$

であるから，題意を得る．□

6.2.3　密度行列の検定

次に，系 $\mathcal{H}$ の密度行列が ρ_0 であるか否かを判定する問題を考えよう．ρ_0 を帰無仮説とよび，真の密度行列が ρ_0 でない場合，想定される密度行列の集合を対立仮説とよび，S_1 と記す．我々が行う判断は，「真の密度行列が ρ_0 である」，「真の密度行列が ρ_0 でない」の 2 つである．以下では，同一の未知状態 ρ の n 階テンソル積状態 $\rho^{\otimes n}$ が与えられた場合について考える．

したがって，$\mathcal{H}^{\otimes n}$ 上の 2 値の測定を行うことになる．前者に対応する POVM 要素を M_0，後者に対応する POVM 要素を M_1 とする．$M_0 + M_1 = I$

であるので，以下では $T_n = M_1$ を用いて我々の判断を記述する．帰無仮説が正しいにも関わらず判断 M_1 を行う確率を第 1 種誤り確率とよび，$\alpha_n(T_n) := \mathrm{Tr}\,\rho_0^{\otimes n} T_n$ で与えられる．帰無仮説が誤っているにも関わらず判断 M_0 を行う確率を第 2 種誤り確率とよび，$\beta_n(T_n) := \max_{\rho \in S_1} \mathrm{Tr}\,\rho^{\otimes n}(I - T_n)$ で与えられる．第 2 種誤り確率が 0 に収束する条件

$$\lim_{n\to\infty} \mathrm{Tr}\,\rho^{\otimes n} T_n = 1$$

の下での第 1 種誤り確率が 0 に収束する指数 $\lim_{n\to\infty} \frac{-1}{n} \log \mathrm{Tr}\,\rho_0^{\otimes n} T_n$ の最大値は $D(\rho\|\rho_0)$ となることが知られている（量子 Stein の補題 [60]）．以下では，ある実数 $R > 0$ の下で任意の $\rho \in S_1$ に対して，$D(\rho\|\rho_0) > R$ となるとき，

$$\lim_{n\to\infty} \frac{-1}{n} \log \mathrm{Tr}\,\rho_0^{\otimes n} T_n = R \tag{6.22}$$

$$\sup_{\rho \in S_1} \lim_{n\to\infty} \mathrm{Tr}\,\rho^{\otimes n} T_n = 1 \tag{6.23}$$

となる検定の系列 $\{T_n\}$ を構成する．この検定の系列は $\rho \in S_1$ に依存していない点にユニバーサル性がある．（量子 Sanov の補題 [8]）．

先に扱った固有値の推定では測定 $\{P_{\boldsymbol{n}}\}$ を用いた．状態の区別には，$\mathcal{W}_{\boldsymbol{n}}$ に含まれる空間 $\mathcal{U}_{\boldsymbol{n}}$ の情報が必要となる．すなわち，空間 $\mathcal{U}_{\boldsymbol{n}}$ 上の測定として，$\mathsf{f}_{\boldsymbol{n}}(\rho)$ と可換となる射影測定で POVM 成分のランクが 1 となるものを選び，$\{P_{\boldsymbol{l}}^{\boldsymbol{n}}\}$ と記す．そして，$\mathcal{H}^{\otimes n}$ 上の射影 $P_{\boldsymbol{n},\boldsymbol{l}} := P_{\boldsymbol{l}}^{\boldsymbol{n}} \otimes I_{\mathcal{V}_{\boldsymbol{n}}}$ に基づく測定 $\{P_{\boldsymbol{n},\boldsymbol{l}}\}$ を考える．この測定によって得られる確率分布を $Q[\rho^{\otimes n}, \rho_0^{\otimes n}](\boldsymbol{n},\boldsymbol{l}) := \mathrm{Tr}\,P_{\boldsymbol{n},\boldsymbol{l}}\rho^{\otimes n}$ とする．この測定と実数 R に基づく検定 T_n を以下で与える．

$$T_n := \sum_{(\boldsymbol{n},\boldsymbol{l}) \in \Omega_n} P_{\boldsymbol{n},\boldsymbol{l}} \tag{6.24}$$

$$\Omega_n := \{(\boldsymbol{n},\boldsymbol{l}) | \log \mathrm{Tr}\,P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho_0) \le -\log \dim \mathcal{V}_{\boldsymbol{n}} - nR\}.$$

すると以下の補題が成り立つ．

補題 6.2.3 (6.24) で定義した T_n は (6.22), (6.23) を満たす．特に，集合 S_1 がコンパクトであるときは，(6.23) において極限と $\sup_{\rho \in S_1}$ の順序交換が可能となり，以下を得る．

$$\lim_{n\to\infty} \max_{\rho \in S_1} \mathrm{Tr}\,\rho^{\otimes n} T_n = 1. \tag{6.25}$$

補題6.2.3の証明に先立って，以下の補題を準備する [40].

補題 6.2.4　確率分布 $Q[\rho^{\otimes n}, \rho_0^{\otimes n}]$ の下で，確率変数 $\frac{1}{n}\log \mathrm{Tr}\, P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho_0)$ および $\frac{1}{n}\log \mathrm{Tr}\, P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho)$ は $\mathrm{Tr}\,\rho\log\rho_0$ および $\mathrm{Tr}\,\rho\log\rho$ に確率収束する.

証明.　$\rho_0^{\otimes n}$ と $P_{\boldsymbol{n},\boldsymbol{l}}$ は可換であるから，

$$\begin{aligned}
&\sum_{\boldsymbol{n},\boldsymbol{l}} \mathrm{Tr}\, P_{\boldsymbol{n},\boldsymbol{l}}\rho^{\otimes n}\left(\frac{1}{n}\log \mathrm{Tr}\, P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho_0) - \mathrm{Tr}\,\rho\log\rho_0\right)^2 \\
&= \mathrm{Tr}\,\rho^{\otimes n}\left(\frac{1}{n}\log \sum_{\boldsymbol{n},\boldsymbol{l}} P_{\boldsymbol{n},\boldsymbol{l}}\rho_0^{\otimes n}P_{\boldsymbol{n},\boldsymbol{l}} - \mathrm{Tr}\,\rho\log\rho_0\right)^2 \\
&= \mathrm{Tr}\,\rho^{\otimes n}\left(\frac{1}{n}\log \rho_0^{\otimes n} - \mathrm{Tr}\,\rho\log\rho_0\right)^2 \\
&= \mathrm{Tr}\,\rho^{\otimes n}\left(\frac{1}{n}(\log \rho_0)^{(n)} - \mathrm{Tr}\,\rho\log\rho_0\right)^2 = \frac{\Delta_\rho^2 \log\rho_0}{n}
\end{aligned} \tag{6.26}$$

となり，$\frac{1}{n}\log \mathrm{Tr}\, P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho_0)$ は $\mathrm{Tr}\,\rho\log\rho_0$ に確率収束する.

一方，$\mathcal{H}^{\otimes n}$ 上の内積 $\mathrm{Tr}\,\rho^{\otimes n}XY$ についての Schwarz の不等式と上記と類似の議論を用いると以下を得る.

$$\begin{aligned}
&\sum_{\boldsymbol{n},\boldsymbol{l}} \mathrm{Tr}\, P_{\boldsymbol{n},\boldsymbol{l}}\rho^{\otimes n}\left(\frac{1}{n}\log \mathrm{Tr}\, P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho) - \mathrm{Tr}\,\rho\log\rho\right)^2 \\
&= \mathrm{Tr}\,\rho^{\otimes n}\left(\frac{1}{n}\log \sum_{\boldsymbol{n},\boldsymbol{l}} P_{\boldsymbol{n},\boldsymbol{l}}\rho^{\otimes n}P_{\boldsymbol{n},\boldsymbol{l}} - \mathrm{Tr}\,\rho\log\rho\right)^2 \\
&\le 2\,\mathrm{Tr}\,\rho^{\otimes n}\left(\frac{1}{n}\log \sum_{\boldsymbol{n},\boldsymbol{l}} P_{\boldsymbol{n},\boldsymbol{l}}\rho^{\otimes n}P_{\boldsymbol{n},\boldsymbol{l}} - \frac{1}{n}\log\rho^{\otimes n}\right)^2 \\
&\quad + 2\,\mathrm{Tr}\, P_{\boldsymbol{n},\boldsymbol{l}}\rho^{\otimes n}P_{\boldsymbol{n},\boldsymbol{l}}\left(\frac{1}{n}\log \rho^{\otimes n} - \mathrm{Tr}\,\rho\log\rho\right)^2 \\
&= 2\frac{1}{n^2}\sum_{\boldsymbol{n}} Q[\rho^{\otimes n}](\boldsymbol{n})\,\mathrm{Tr}\,\mathsf{f}_{\boldsymbol{n}}(\rho)\left(\log\sum_{\boldsymbol{l}} P_{\boldsymbol{l}}^{\boldsymbol{n}}\mathsf{f}_{\boldsymbol{n}}(\rho)P_{\boldsymbol{l}}^{\boldsymbol{n}} - \log\mathsf{f}_{\boldsymbol{n}}(\rho)\right)^2 \\
&\quad + \frac{2\Delta_\rho^2\log\rho}{n}
\end{aligned}$$

$$\leq \frac{4}{n^2} \max_{\boldsymbol{n} \in \mathcal{Y}_n^r} (\log \dim \mathcal{U}_{\boldsymbol{n}})^2 + \frac{2\Delta_\rho^2 \log \rho}{n} \tag{6.27}$$

$$\leq \frac{r^2(r-1)^2(\log(n+1))^2}{n^2} + \frac{2\Delta_\rho^2 \log \rho}{n}. \tag{6.28}$$

不等式 (6.27), (6.28) の導出では (2.28), (6.12) をそれぞれ用いた．(6.27) の右辺の値は 0 に収束するので，確率分布 $Q[\rho^{\otimes n}, \rho_0^{\otimes n}]$ の下で，確率変数 $\frac{1}{n} \log \operatorname{Tr} P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho)$ は $\operatorname{Tr} \rho \log \rho$ に確率収束する． □

補題 6.2.3 の証明． Ω_n の定義より，$(\boldsymbol{n}, \boldsymbol{l}) \in \Omega_n$ について，$\operatorname{Tr} \rho_0^{\otimes n} P_{\boldsymbol{n},\boldsymbol{l}} \leq e^{-nR}$ となる．したがって，(6.12), (6.14) を用いることで，

$$\begin{aligned} \operatorname{Tr} \rho^{\otimes n} T_n &= \sum_{(\boldsymbol{n},\boldsymbol{l}) \in \Omega_n} \operatorname{Tr} \rho_0^{\otimes n} P_{\boldsymbol{n},\boldsymbol{l}} \leq \sum_{(\boldsymbol{n},\boldsymbol{l}) \in \Omega_n} e^{-nR} \\ &\leq |\mathcal{Y}_n^r| \cdot \max_{\boldsymbol{n} \in \mathcal{Y}_n^r} \dim \mathcal{U}_{\boldsymbol{n}} \cdot e^{-nR} \leq (n+1)^{r(r-1)/2+r-1} e^{-nR} \end{aligned}$$

を得る．よって，(6.22) を得る．

$\rho \in S_1$ に対して，$\Omega[\rho]_n$ を以下で定義する．

$$\Omega[\rho]_n := \{(\boldsymbol{n}, \boldsymbol{l}) | \log \operatorname{Tr} P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho_0) - \log \operatorname{Tr} P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho) \leq -nR\}.$$

$\dim \mathcal{V}_{\boldsymbol{n}} \operatorname{Tr} P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho) \leq 1$ であるから，$\Omega[\rho]_n$ の条件式が成り立つときは Ω_n の条件式が成り立つ．すなわち，$\Omega[\rho]_n \subset \Omega_n$ となる．したがって，

$$\sum_{(\boldsymbol{n},\boldsymbol{l}) \in \Omega[\rho]_n} \operatorname{Tr} \rho^{\otimes n} P_{\boldsymbol{n},\boldsymbol{l}} \to 1 \tag{6.29}$$

を示せば十分である．確率変数 $\log \operatorname{Tr} P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho_0) - \log \operatorname{Tr} P_{\boldsymbol{l}}^{\boldsymbol{n}} \mathsf{f}_{\boldsymbol{n}}(\rho)$ は補題 6.2.4 より，$D(\rho \| \rho_0)$ に確率収束するので，(6.29) が成り立つ．よって，(6.23) を得る．

特に，集合 S_1 がコンパクトであるときは，$R_0 := \max_{\rho \in S_1} D(\rho \| \rho_0) < R$ であるので，Markov の不等式（補題 2.3.7）より，

$$Q[\rho^{\otimes n}, \rho_0^{\otimes n}] {\Omega[\rho]_n}^c$$

$$\le Q\left[\frac{\mathrm{E}_{Q[\rho^{\otimes n},\rho_0^{\otimes n}]}(\frac{1}{n}\log \mathrm{Tr}\, P^{\boldsymbol{n}}_{\boldsymbol{l}}\mathsf{f}_{\boldsymbol{n}}(\rho_0)-\frac{1}{n}\log \mathrm{Tr}\, P^{\boldsymbol{n}}_{\boldsymbol{l}}\mathsf{f}_{\boldsymbol{n}}(\rho)-D(\rho\|\rho_0))^2}{(R-D(\rho\|\rho_0))^2}\right]$$

$$\le \frac{\frac{2\Delta_\rho^2\log\rho_0}{n}+\frac{2r^2(r-1)^2(\log(n+1))^2}{n^2}+\frac{4\Delta_\rho^2\log\rho}{n}}{(R-R_0)^2} \tag{6.30}$$

を得る．最後の不等式では補題6.2.4の証明での不等式(6.28), (6.26)および，補題2.3.8を用いた．(6.30)は$\rho\in S_1$に依存しないので，(6.25)を得る．　□

6.2.4　測定値から定まるエントロピーの振る舞い

(6.16), (6.17), (6.12)より，$n\to\infty$の極限においては，$\frac{1}{n}\log(\dim\mathcal{V}_{\boldsymbol{n}})$および$\frac{1}{n}\log(\mathrm{rank}\,P_{\boldsymbol{n}})$は$H(\frac{\boldsymbol{n}}{n})$に一致する．本項では，確率分布$Q[\rho^{\otimes n}]$の下でのこれらの値の確率変数としての振る舞いを扱う．補題6.2.1より，$H(\frac{\boldsymbol{n}}{n})$などの上記の確率変数は$H(\boldsymbol{p})$に確率収束する．特に，補題6.2.2より，$\epsilon_n$が$\sqrt{n}\epsilon_n\to\infty$を満たすとき，$|H(\frac{\boldsymbol{n}}{n})-H(\boldsymbol{p})|\le\epsilon_n$となる確率は1に収束する．したがって，これら確率変数の期待値は$H(\boldsymbol{p})$に収束する．しかし，これらの期待値が$H(\boldsymbol{p})$に収束する速さは確率変数ごとに異なる．$\log(\dim\mathcal{V}_{\boldsymbol{n}})$の期待値の漸近的な振る舞いは以下の補題で与えられる[85].

補題 6.2.5　確率変数$\log(\dim\mathcal{V}_{\boldsymbol{n}})$確率分布$Q[\rho^{\otimes n}]$の下での期待値の漸近的な振る舞いは以下で与えられる．

$$\lim_{n\to\infty}\sum_{\boldsymbol{n}}Q[\rho^{\otimes n}](\boldsymbol{n})\log(\dim\mathcal{V}_{\boldsymbol{n}})-nH(\boldsymbol{p})+\frac{r-1}{2}\log n$$
$$=-\frac{r-1}{2}\log 2\pi e-\frac{1}{2}\sum_{j=1}^{r}\log p_j+\log\prod_{i,j:i<j}(p_i-p_j)$$
$$-\frac{\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\prod_i p_i^{\delta_{\sigma(i)}}\log\prod_j p_j^{\delta_{\sigma(k)}}}{\prod_{i,j:i<j}(p_i-p_j)}. \tag{6.31}$$

証明.　初めに，補題6.2.1の証明で与えられた$\sigma\in S_r$に応じて決まる確率分布$\mathrm{Mul}[\boldsymbol{p},n,\sigma](\boldsymbol{n}):=\prod_{l=1}^r a_l^{n_l^\sigma}\frac{n!}{\boldsymbol{n}^\sigma!}$の下で，確率変数$\log(\dim\mathcal{V}_{\boldsymbol{n}})$の期待値を求める．

$$
\begin{aligned}
\log(\dim \mathcal{V}_{\boldsymbol{n}}) &= \log\left\{\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\frac{n!}{[\boldsymbol{n}+\boldsymbol{\delta}-\sigma'(\boldsymbol{\delta})]!}\right\} \\
&= \log\left\{\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\frac{n!}{[\boldsymbol{n}^\sigma+\sigma(\delta)-\sigma'(\boldsymbol{\delta})]!}\right\} \\
&= \log\frac{n!}{\boldsymbol{n}^\sigma!}+\log\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\frac{\boldsymbol{n}^\sigma!}{[\boldsymbol{n}^\sigma+\sigma(\delta)-\sigma'(\boldsymbol{\delta})]!}. \qquad (6.32)
\end{aligned}
$$

すると，(6.32) の第 1 項の期待値は補題 6.1.4 で与えたものとなる．一方，確率分布 $\prod_{l=1}^r a_l^{n_l^\sigma}\frac{n!}{\boldsymbol{n}^\sigma!}$ の下で，(6.32) の第 2 項は以下の値に確率収束する．

$$
\begin{aligned}
&\log\sum_{\sigma'\in S_r,} \operatorname{sgn}(\sigma')\frac{\boldsymbol{n}^\sigma!}{[\boldsymbol{n}^\sigma+\sigma(\delta)-\sigma'(\boldsymbol{\delta})]!} \\
&= \log\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\frac{\prod_{i:\delta_{\sigma(i)}-\delta_{\sigma'(i)}<0}\prod_{j=1}^{\delta_{\sigma(i)}-\delta_{\sigma'(i)}}(n_i^\sigma-j+1)}{\prod_{i:\delta_{\sigma(i)}-\delta_{\sigma'(i)}>0}\prod_{j=1}^{\delta_{\sigma'(i)}-\delta_{\sigma(i)}}(n_i^\sigma+j)} \\
&= \log\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\frac{\prod_{i:\delta_{\sigma(i)}-\delta_{\sigma'(i)}<0}\prod_{j=1}^{\delta_{\sigma(i)}-\delta_{\sigma'(i)}}\frac{n_i^\sigma-j+1}{n}}{\prod_{i:\delta_{\sigma(i)}-\delta_{\sigma'(i)}>0}\prod_{j=1}^{\delta_{\sigma'(i)}-\delta_{\sigma(i)}}\frac{n_i^\sigma+j}{n}} \\
&\to \log\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\frac{\prod_{i:\delta_{\sigma(i)}-\delta_{\sigma'(i)}<0}p_i^{\delta_{\sigma'(i)}-\delta_{\sigma(i)}}}{\prod_{i:\delta_{\sigma(i)}-\delta_{\sigma'(i)}>0}p_i^{\delta_{\sigma(i)}-\delta_{\sigma'(i)}}} \\
&= \log\sum_{\sigma'\in S_r} \operatorname{sgn}(\sigma')\prod_i p_i^{\delta_{\sigma'(i)}-\delta_{\sigma(i)}} = \log\prod_{i,j:i<j}(p_i-p_j)\prod_j p_j^{-\delta_{\sigma(j)}} \\
&= \log\prod_{i,j:i<j}(p_i-p_j)-\log\prod_j p_j^{\delta_{\sigma(j)}}.
\end{aligned}
$$

ここで，Vandermonde の行列式を用いた．したがって，これまでの議論を整理すると，

$$
\begin{aligned}
&\mathrm{E}_{\mathrm{Mul}[\boldsymbol{p},n,\sigma]}\log(\dim \mathcal{V}_{\boldsymbol{n}})-nH(\boldsymbol{p})+\frac{r-1}{2}\log n \\
&\to -\frac{r-1}{2}\log 2\pi e-\frac{1}{2}\sum_{j=1}^r\log p_j+\log\prod_{i,j:i<j}(p_i-p_j)-\log\prod_j p_j^{\delta_{\sigma(j)}}
\end{aligned}
\qquad (6.33)
$$

を得る．

さらに，補題 6.2.1 の証明での議論から，確率分布 $\prod_{l=1}^r a_l^{n_l^\sigma} \frac{n!}{\boldsymbol{n}^\sigma!}$ の下での (6.33) の期待値について，係数 $\frac{\mathrm{sgn}(\sigma)\prod_i p_i^{\delta_{\sigma(i)}}}{\prod_{i,j:i<j}(p_i-p_j)}$ を持つ重み和をとれば，求めたい値に一致する．(6.33) の最終項以外は，σ に依存しないので，(6.21) に注意すると，(6.31) を得る．　□

6.3　量子2準位系の状態推定

6.2.2 項では密度行列の固有値のみを推定する問題を扱った．以下では，量子系が $\mathbb{C}^2$ の場合に，固有値に加え，ユニタリ方向の情報も推定し，密度行列の形を完全に決定する問題を扱う．したがって，パラメータ空間は $\mathbb{C}^2$ 上の密度行列の集合となる．6.2.2 項で与えた測定 $\{P_{\boldsymbol{n}}\}$ を行い，その後，各既約成分でユニタリ方向の推定を行う．1 段階目での測定の測定値が $\boldsymbol{n}$ とすると，系 $\mathcal{W}_{\boldsymbol{n}}$ 上の測定を行うことになる．このとき系の状態は $\mathsf{f}_{\boldsymbol{n}}(\rho)\otimes I_{\mathcal{V}_{\boldsymbol{n}}}$ である．この場合，系 $\mathcal{V}_{\boldsymbol{n}}$ には，情報がないので，この系について部分トレースをとっても，情報の損失はない．したがって，系 $\mathcal{U}_{\boldsymbol{n}}$ 上の状態 $\mathsf{f}_{\boldsymbol{n}}(\rho)$ を推定する問題となる．1 段階目での測定で固有値がほぼわかっている．固有値が既知であるとして，ユニタリ方向の情報のみを推定する問題であれば，4.2 節の例 4.2.6 で扱った問題と一致する．したがって，2 段階目の測定として最高ウェイトベクトル $|\frac{n_1-n_2}{2},\frac{n_1-n_2}{2}\rangle$ が生成する POVM を選ぶ．測定 $M_{\boldsymbol{n},\zeta} := \mathsf{f}_{\boldsymbol{n}}(g(\zeta))|\frac{n_1-n_2}{2};\frac{n_1-n_2}{2}\rangle\langle\frac{n_1-n_2}{2};\frac{n_1-n_2}{2}|\mathsf{f}_{\boldsymbol{n}}(g(\zeta))^\dagger\otimes I_{\mathcal{V}_{\boldsymbol{n}}} = |\frac{n_1-n_2}{2}:\zeta\rangle\langle\frac{n_1-n_2}{2}:\zeta|\otimes I_{\mathcal{V}_{\boldsymbol{n}}}$ を行い，推定値として，$g(\zeta)\rho(\frac{\boldsymbol{n}}{n})g(\zeta)^\dagger$ を与える方法を行うことにする．ここで，$\rho(\boldsymbol{n})$ を不変にする固定化群 H で割った商空間を $\mathrm{SU}(2)/H$ とし，$\zeta\in\mathrm{SU}(2)/H$ の代表元を $g(\zeta)$ とした．

したがって，真の状態 ρ と推定値 $g(\zeta)\rho(\frac{\boldsymbol{n}}{n})g(\zeta)^\dagger$ との $F(\rho, g(\zeta)\rho(\frac{\boldsymbol{n}}{n})g(\zeta)^\dagger)$ の平均値は以下で与えられる．以下では，ρ が対角行列の場合を扱い，$\rho=\rho_{(r,0,0)}=c_1e^{tE_{0,1}}$ となるように r,t,c_1 を選ぶ．$c(\lambda)=\frac{e^t-1}{e^{t(\lambda+1)}-e^{-t\lambda}}$ とすると，(4.27) より，

$$\sum_{\boldsymbol{n}\in\mathcal{Y}_n^2}\int_{S^2}F\left(\rho, g(\zeta)\rho\left(\frac{\boldsymbol{n}}{n}\right)g(\zeta)^\dagger\right)^2\mathrm{Tr}\,\rho^{\otimes n}M_{\boldsymbol{n},\theta}\mu_{S^2}(d\zeta)$$

$$
\begin{aligned}
&= \sum_{k=0}^{\lfloor n/2 \rfloor} Q[\rho^{\otimes n}]\left(\frac{n-k}{n}, \frac{k}{n}\right) \\
&\quad \cdot \int_{S^2} F\left(\rho, g(\zeta)\rho\left(\frac{n-k}{n}, \frac{k}{n}\right) g(\zeta)^{\dagger}\right)^2 c\left(\frac{n-2k}{2}\right) \\
&\quad \cdot \left\langle \frac{n-2k}{2} : \zeta \middle| e^{tf_{\frac{n-2k}{2}}(E_{0,1})} \middle| \frac{n-2k}{2} : \zeta \right\rangle \mu_{S^2}(d\zeta) \\
&= \sum_{k=0}^{\lfloor n/2 \rfloor} Q[\rho^{\otimes n}]\left(\frac{n-k}{n}, \frac{k}{n}\right) \\
&\quad \cdot \left(\frac{1}{2} + \frac{n-2k}{n}\left(\frac{(n-2k+1)((1+r)^{n-2k+2}-(1-r)^{n-2k+2})}{2(n-2k+2)((1+r)^{n-2k+1}-(1-r)^{n-2k+1})} - \frac{1}{2}\right)\right. \\
&\qquad \left. + \sqrt{1-\left(\frac{n-2k}{n}\right)^2}\frac{\sqrt{1-r^2}}{2}\right) \qquad (6.34)
\end{aligned}
$$

を得る．補題6.2.2より，$\frac{n-2k}{n}$ の期待値が $r + \frac{K}{n} + o(\frac{1}{n})$ となるように K を選ぶ．すると，$\frac{1}{2} + \frac{n-2k}{n}\left(\frac{(n-2k+1)((1+r)^{n-2k+2}-(1-r)^{n-2k+2})}{2(n-2k+2)((1+r)^{n-2k+1}-(1-r)^{n-2k+1})} - \frac{1}{2}\right)$ の期待値は，$\frac{1-r^2}{2} + \frac{r}{2}\frac{K}{n} - \frac{1+r}{2n} + o(\frac{1}{n})$ となる．一方，$\Delta(r) := \frac{n-2k}{n} - r$ とすると，

$$
\sqrt{1-(\frac{n-2k}{n})^2}\frac{\sqrt{1-r^2}}{2} = \frac{1-r^2}{2} - \frac{r}{2}\Delta(r) - \frac{1}{4(1-r^2)}\Delta(r)^2 + o(\Delta(r)^2) \tag{6.35}
$$

となる．$\Delta(r)^2$ の期待値は $\frac{1-r^2}{n}$ となるので，(6.35) の期待値は $\frac{1-r^2}{2} - \frac{r}{2}\frac{K}{n} - \frac{1}{4n} + o(\frac{1}{n})$ となる．すなわち，(6.34) は $1 - \frac{3+2r}{4n} + o(\frac{1}{n})$ となる [42, 2]．

6.4 ユニバーサルな量子状態の近似

2.4節で与えた2状態 ρ_1, ρ_2 の相違の度合いを表す関数 $f(\rho_1, \rho_2)$ のうちテンソル積に関して加法性が成り立つものについてユニバーサルな量子状態の近似を考える．この概念は，ユニバーサルな情報処理のカギとなる考え方である．以下では，関数 $f(\rho_1, \rho_2)$ の下での状態の集合 $\mathcal{S}$ に対する近似を考える．$\mathcal{H}^{\otimes n}$ 上の状態 ρ_n の系列 $\{\rho_n\}$ が以下を満たすとき，$\{\rho_n\}$ を f の下での $\mathcal{S}$

に対する**ユニバーサルな近似**という.

$$\lim_{n\to\infty}\frac{1}{n}f(\rho^{\otimes n},\rho_n)=0,\quad \forall\rho\in\mathcal{S}.$$

なお，f が距離の公理を満たすか，距離の公理を満たす関数の狭義単調増加関数で表されるとき，ユニバーサルな近似となる状態の系列は存在しない．本節では，ユニバーサルな近似となる例を紹介し，後の節の準備とする．

例えば，$\mathcal{H}=\mathbb{C}^r$ のとき，$\rho_{\boldsymbol{n}}:=\frac{1}{\dim\mathcal{W}_{\boldsymbol{n}}}P(\mathcal{W}_{\boldsymbol{n}})$ と $\rho_{U,n}:=\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r}\frac{1}{|\mathcal{Y}_n^r|}\rho_{\boldsymbol{n}}$ を定義すると，

$$[\rho_{U,n}\otimes\rho_{U,m},\rho_{U,n+m}]=0 \tag{6.36}$$

が成り立つ．この事実は，$S_n\times S_m$ が置換群 S_{n+m} の部分群であることから確認できる．さらに，以下の定理が成り立つ [48].

定理 6.4.1　状態の系列 $\{\rho_{U,n}\}$ は

$$D_{\max}(\rho^{\otimes n}\|\rho_{U,n})\le\frac{(r+2)(r-1)}{2}\log(n+1) \tag{6.37}$$

を満たす．したがって，相対 Max エントロピーの下での $\mathcal{S}(\mathcal{H})$ に対するユニバーサルな近似となる.

証明.　$\frac{\dim\mathcal{U}_{\boldsymbol{n}}}{\dim\mathcal{W}_{\boldsymbol{n}}}P(\mathcal{W}_{\boldsymbol{n}})\ge P(\mathcal{W}_{\boldsymbol{n}})\rho^{\otimes n}P(\mathcal{W}_{\boldsymbol{n}})$ となることから，行列不等式 $|\mathcal{Y}_n^r|\max_{\boldsymbol{n}\in\mathcal{Y}_n^r}\dim\mathcal{U}_{\boldsymbol{n}}\rho_{U,n}\ge\rho^{\otimes n}$ を得る．(6.12), (6.14) より，$|\mathcal{Y}_n^r|\max_{\boldsymbol{n}\in\mathcal{Y}_n^r}\dim\mathcal{U}_{\boldsymbol{n}}\le(n+1)^{(r+2)(r-1)/2}$ が成り立つので，(6.37) を得る．□

さらに，相対エントロピーについては以下の定理が成り立つ [47].

定理 6.4.2　ρ の固有値からなる確率分布を $\boldsymbol{p}$ とするとき，状態の系列 $\{\rho_{U,n}\}$ は

$$D(\rho^{\otimes n}\|\rho_{U,n})=\frac{r^2-1}{2}\log n+C_r-\log r!(r-1)!+C(\boldsymbol{p})+o(1) \tag{6.38}$$

を満たす．ここで，C_r, $C(\boldsymbol{p})$ を以下で定義した.

$$C_r:=-\frac{r-1}{2}\log 2\pi e-\sum_{j=1}^{r}(r-j)\log j$$

$$C(\boldsymbol{p}) := -\sum_{\sigma \in S_r} \frac{\operatorname{sgn}(\sigma)(\prod_j p_j^{\delta_{\sigma(j)}}) \log(\prod_j p_j^{\delta_{\sigma(j)}})}{\prod_{i<j}(p_i - p_j)} + 2\log \prod_{i<j}(p_i - p_j) - \frac{1}{2}\sum_j \log p_j.$$

証明.

$$D(\rho^{\otimes n}\|\rho_{U,n}) = -\operatorname{Tr} \rho^{\otimes n} \log \rho_{U,n} - nH(\boldsymbol{p})$$
$$= \sum_{\boldsymbol{n} \in \mathcal{Y}_n^r} Q[\rho^{\otimes n}](\boldsymbol{n})(\log|\mathcal{Y}_n^r| + \log \dim \mathcal{U}_{\boldsymbol{n}} + \log \dim \mathcal{V}_{\boldsymbol{n}}) - nH(\boldsymbol{p}) \quad (6.39)$$

を満たす．(6.13) より，

$$\sum_{\boldsymbol{n} \in \mathcal{Y}_n^r} Q[\rho^{\otimes n}](\boldsymbol{n}) \log \dim \mathcal{V}_{\boldsymbol{n}}$$
$$= (r-1)\log n + \sum_{j<l} \log(p_l - p_j) - \sum_{j=1}^{r}(r-j)\log j + o(1) \quad (6.40)$$

となる．したがって，(6.39), (6.40) に (6.15), (6.31) を加えることで (6.38) を得る． □

相対エントロピーの下のユニバーサルな近似について min-max の意味で最適化を考えることができる．すなわち，(6.38) の右辺の定数項の部分の最悪の場合の最適化は以下のように定式化できる．

$$D_{\text{min-max}}(r) := \min_{\{\sigma_n\}} \sup_{\rho} \lim_{n\to\infty} D(\rho^{\otimes n}\|\sigma_n) - \frac{r^2-1}{2}\log n. \quad (6.41)$$

この量について以下の定理が成り立つ [47].

定理 6.4.3 最小値 $D_{\text{min-max}}(r)$ は σ_n が $\sigma_{J,n} := \sum_{\boldsymbol{n} \in \mathcal{Y}_n^r} \frac{J_n(\boldsymbol{n})}{\dim \mathcal{W}_{\boldsymbol{n}}} P(\mathcal{W}_{\boldsymbol{n}})$ または，$\tilde{\sigma}_{J,n} := \int_{\mathcal{Y}(r)} \int_{\mathrm{SU}(r)} (U\rho(\boldsymbol{p})U^\dagger)^{\otimes n} \mu(dU) J(\boldsymbol{p}) d\boldsymbol{p}$ のとき，達成し，$D_{\text{min-max}}(r) = C_r + \log \int_{\mathcal{Y}_r} e^{C(\boldsymbol{p})} d\boldsymbol{p}$ が成り立つ．ただし，$J_n(\boldsymbol{n}) := \frac{e^{C(\frac{\boldsymbol{n}}{n})}}{\sum_{\boldsymbol{n}' \in \mathcal{Y}_n^r} e^{C(\frac{\boldsymbol{n}'}{n})}}$, $J(\boldsymbol{p}) := \frac{e^{C(\boldsymbol{p})}}{\int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p})} d\boldsymbol{p}}$ である．

古典系では，上記の mini-max を実現する ρ_n はパラメータ付き分布の n 次の独立同一分布をパラメータに関する Jeffreys 事前分布で平均したものである．したがって，密度行列上の確率分布 $\mu(dU)J(\boldsymbol{p})d\boldsymbol{p}$ は密度行列の集合上の確率分布と見なすことができる．この確率分布は，ある意味で，Jeffreys 事前分布の量子版と見なすことができる．

証明.　密度行列 $\rho^{\otimes n}$ は [37] の (4.43) で与えた置換群 S_n の表現 f_n に関して不変であるから, $g \in S_n$ について, $D(\rho^{\otimes n}\|\sigma_n) = -\operatorname{Tr}[\rho^{\otimes n}\log\sigma_n] - nH(\rho)$ は $-\operatorname{Tr}[\rho^{\otimes n}\log \mathsf{f}_n(g)\sigma_n\mathsf{f}_n(g)^\dagger] - nH(\rho)$ に等しい．したがって, 関数 $x \mapsto -\log x$ が行列凸であることから，以下を得る．

$$
\begin{aligned}
&-\operatorname{Tr}[\rho^{\otimes n}\log\sigma_n] - nH(\rho) \\
&= \sum_{g\in S_n}\frac{1}{|S_n|}\operatorname{Tr}[\rho^{\otimes n}(-\log \mathsf{f}_n(g)\sigma_n\mathsf{f}_n(g)^\dagger)] - nH(\rho) \\
&\ge -\operatorname{Tr}\left[\rho^{\otimes n}\log\sum_{g\in S_n}\frac{1}{|S_n|}\mathsf{f}_n(g)\sigma_n\mathsf{f}_n(g)^\dagger\right] - nH(\rho).
\end{aligned}
$$

密度行列 $\sum_{g\in S_n}\frac{1}{|S_n|}\mathsf{f}_n(g)\sigma_n\mathsf{f}_n(g)^\dagger$ は置換群 S_n の作用に関して不変であるので，(6.41) における密度行列 σ_n を置換群 S_n の作用に関して不変なものに制限できる．

関数 $x \mapsto -\log x$ の作用素凸性より，$\mathrm{SU}(r)$ 上の不変測度 μ は以下を満たす．

$$
\begin{aligned}
&\sup_{\rho}\varlimsup_{n\to\infty}\left(D(\rho^{\otimes n}\|\sigma_n) - \frac{r^2-1}{2}\log n\right) \\
&= \sup_{\boldsymbol{p}}\sup_{U\in\mathrm{SU}(r)}\varlimsup_{n\to\infty} -\operatorname{Tr}\rho(\boldsymbol{p})^{\otimes n}\log\left[U^{\otimes n}\sigma_n U^{\otimes n\dagger}\right] - nH(\boldsymbol{p}) - \frac{r^2-1}{2}\log n \\
&\ge \sup_{\boldsymbol{p}}\varlimsup_{n\to\infty} -\int_{\mathrm{SU}(r)}\operatorname{Tr}\rho(\boldsymbol{p})^{\otimes n}\log\left[U^{\otimes n}\sigma_n U^{\otimes n\dagger}\right]\mu(dU) \\
&\quad - nH(\boldsymbol{p}) - \frac{r^2-1}{2}\log n \\
&= \sup_{\boldsymbol{p}}\varlimsup_{n\to\infty} -\operatorname{Tr}\rho(\boldsymbol{p})^{\otimes n}\left[\int_{\mathrm{SU}(r)}\log\left[U^{\otimes n}\sigma_n U^{\otimes n\dagger}\right]\mu(dU)\right]
\end{aligned}
$$

$$
\begin{aligned}
&- nH(\boldsymbol{p}) - \frac{r^2-1}{2}\log n \\
\geq &\sup_{\boldsymbol{p}} \lim_{n\to\infty} -\mathrm{Tr}\,\rho(\boldsymbol{p})^{\otimes n} \log \left(\int_{\mathrm{SU}(r)} U^{\otimes n}\sigma_n U^{\otimes n\dagger}\mu(dU) \right) \\
&- nH(\boldsymbol{p}) - \frac{r^2-1}{2}\log n.
\end{aligned}
$$

密度行列 $\left(\int_{\mathrm{SU}(r)} U^{\otimes n}\sigma_n U^{\otimes n\dagger}\mu(dU)\right)$ は $\mathrm{SU}(r)$ の作用に関して不変であるので，(6.41) における密度行列 σ_n を $\mathrm{SU}(r)$ の作用に関して不変なものに限ることができる．したがって，以下を得る．

$$
\begin{aligned}
&\inf_{\{\sigma_n\}} \sup_{\rho} \overline{\lim_{n\to\infty}} \left(D(\rho^{\otimes n}\|\sigma_n) - \frac{r^2-1}{2}\log n \right) \\
&= \inf_{\{P_n\}} \sup_{\rho} \overline{\lim_{n\to\infty}} \left(D(\rho^{\otimes n}\|\sigma_{P_n,n}) - \frac{r^2-1}{2}\log n \right),
\end{aligned}
$$

ここで，P_n は $\mathcal{Y}_n^r$ 上の確率分布であり，$\sigma_{P_n,n} := \sum_{\boldsymbol{n}\in\mathcal{Y}_n^r} P_n(\boldsymbol{n})\rho_{\boldsymbol{n}}$ とした．

さらに，$\frac{\sum_{\boldsymbol{n}'\in\mathcal{Y}_n^r} e^{C(\frac{\boldsymbol{n}'}{n})}}{n^{r-1}} \to \int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p})}d\boldsymbol{p}$ であるから，以下を得る．

$$
\begin{aligned}
&D(\rho(\boldsymbol{p})^{\otimes n}\|\sigma_{P_n,n}) \\
&\cong \frac{r^2-1}{2}\log n + C_r - \log r!(r-1)! + C(\boldsymbol{p}) - \log \frac{P_n(\boldsymbol{n})}{\frac{1}{|\mathcal{Y}_n^r|}} \\
&\cong \frac{r^2-1}{2}\log n + C_r - \log r!(r-1)! + \log \left(\int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p}')}d\boldsymbol{p}' \right) \\
&\quad + \log J(\boldsymbol{p}) - \sum_{\boldsymbol{n}} Q_{\boldsymbol{p}}(\boldsymbol{n}) \log P_n(\boldsymbol{n}) \frac{n^{r-1}}{r!(r-1)!} \\
&\cong \frac{r^2-1}{2}\log n + C_r + \log \int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p}')}d\boldsymbol{p}' \\
&\quad + \sum_{\boldsymbol{n}} Q_{\boldsymbol{p}}(\boldsymbol{n})(\log J(\boldsymbol{p}) - \log P_n(\boldsymbol{n}) - (r-1)\log n). \qquad (6.42)
\end{aligned}
$$

(6.42) の最終項のみが $\boldsymbol{p}$ に依存する．この最終項を評価するために，結合分布 $Q_{J,n}(\boldsymbol{p},\boldsymbol{n}) := J(\boldsymbol{p})Q_{\boldsymbol{p}}(\boldsymbol{n})$ を考える．

補題6.2.1より，確率分布 $Q_{\boldsymbol{p}}$ の下で確率変数 $\frac{\boldsymbol{n}}{n}$ は $\boldsymbol{p}$ に確率収束し，$J(\boldsymbol{p})$ が連続であることから，周辺分布 $Q_{J,n}(\boldsymbol{n})(=\int_{\mathcal{Y}(r)} Q_{J,n}(\boldsymbol{p},\boldsymbol{n})d\boldsymbol{p})$ は $J_n(\boldsymbol{n})$ に近づく．条件付き確率 $Q_{J,n}(\boldsymbol{p}|\boldsymbol{n})$ の下で，確率変数 $\boldsymbol{p}$ は $\frac{\boldsymbol{n}}{n}$ に確率収束する．よって，以下を得る．

$$\int_{\mathcal{Y}(r)} \log J(\boldsymbol{p}) \frac{Q_{\boldsymbol{p}}(\boldsymbol{n}) J_n(\boldsymbol{p})}{\int_{\mathcal{Y}(r)} J_n(\boldsymbol{p}) \mathrm{P}_{\boldsymbol{p}}(\boldsymbol{n}) d\boldsymbol{p}} d\boldsymbol{p} \cong \log J\left(\frac{\boldsymbol{n}}{n}\right) \tag{6.43}$$

$$= \log J_n(\boldsymbol{n}) + \log \frac{\sum_{\boldsymbol{n}' \in \mathcal{Y}_n^r} e^{C(\frac{\boldsymbol{n}'}{n})}}{\int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p})} d\boldsymbol{p}} \cong \log J_n(\boldsymbol{n}) + (r-1)\log n. \tag{6.44}$$

一方，確率分布 $Q_{\boldsymbol{p}}(\boldsymbol{n})$ の下で確率変数 $\frac{\boldsymbol{n}}{n}$ は $\boldsymbol{p}$ に確率収束することから，同じ確率分布 $Q_{\boldsymbol{p}}(\boldsymbol{n})$ の下で確率変数 $\log J_n(\boldsymbol{n}) - (r-1)\log n$ は $\log J(\boldsymbol{p})$ に確率収束する．すなわち，任意の $\boldsymbol{p}$ について

$$\sum_{\boldsymbol{n}} Q_{\boldsymbol{p}}(\boldsymbol{n})(\log J(\boldsymbol{p}) - \log J_n(\boldsymbol{n}) - (r-1)\log n) \to 0 \tag{6.45}$$

が成り立つ．

(6.44)を用いて，(6.42)の最終項を $\boldsymbol{p}$ について最大化を考えると以下を得る．

$$\begin{aligned}
&\sup_{\boldsymbol{p}} \sum_{\boldsymbol{n}} Q_{\boldsymbol{p}}(\boldsymbol{n})(\log J(\boldsymbol{p}) - \log P_n(\boldsymbol{n}) - (r-1)\log n) \\
&\geq \int_{\mathcal{Y}(r)} \sum_{\boldsymbol{n}} Q_{\boldsymbol{p}}(\boldsymbol{n})(\log J(\boldsymbol{p}) - \log P_n(\boldsymbol{n}) - (r-1)\log n) J(\boldsymbol{p}) d\boldsymbol{p} \\
&\cong \sum_{\boldsymbol{n}} J_n(\boldsymbol{n})(\log J_n(\boldsymbol{n}) - \log P_n(\boldsymbol{n})) = D(J_n \| P_n) \geq 0.
\end{aligned}$$

よって，

$$\begin{aligned}
&\lim_{n\to\infty} \sum_{\boldsymbol{n}} P_n(\boldsymbol{n}) \left(D\left(\rho(\frac{\boldsymbol{n}}{n})^{\otimes n} \| \sigma_{P_n,n} \right) - \frac{r^2-1}{2} \log n \right) \\
&\geq C_r + \log \int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p})} d\boldsymbol{p}
\end{aligned}$$

となる．(6.45)より，上記の等号は $P_n(\boldsymbol{n}) = J_n(\boldsymbol{n})$ となるときに成立する．したがって，

$$\min_{\{\sigma_n\}} \sup_{\rho} \lim_{n\to\infty} \left(D(\rho^{\otimes n} \| \sigma_n) - \frac{r^2-1}{2} \log n \right) = C_r + \log \int_{\mathcal{Y}(r)} e^{C(\boldsymbol{p})} d\boldsymbol{p}$$

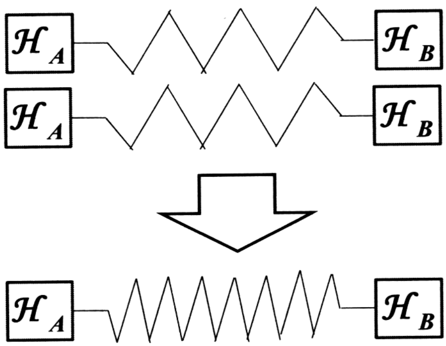


図 6.1 エンタングルメント集中化

を得る．密度行列 $\overline{\rho(\boldsymbol{p})^{\otimes n}}$ は $\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r} Q_{\boldsymbol{p}}(\boldsymbol{n})\rho_{\boldsymbol{n}}$ と書けることから，密度行列 $\tilde{\sigma}_{J,n}$ は $\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r} Q_{J,n}(\boldsymbol{n})\rho_{\boldsymbol{n}}$ と書ける．$Q_{J,n}(\boldsymbol{n})$ は $J_n(\boldsymbol{n})$ に収束することから，密度行列 $\tilde{\sigma}_{J,n}$ も (6.41) における mini-max の値を達成する． □

6.5 エンタングルメント集中化

6.5.1 縮約密度行列の基底が既知の場合

3.2 節などで紹介した量子テレポーテーションなどの量子プロトコルのためには，最大エンタングル状態が必要となる．しかし，一般には，完全なエンタングル状態を生成することは困難であることが多く，不完全なエンタングル状態しか生成されないことが多い．複数の不完全なエンタングル状態から完全なエンタングル状態を生成するプロトコルを**エンタングルメント蒸留**という．特に，最初に与えられた不完全なエンタングル状態が純粋状態のとき，エンタングルメント蒸留は**エンタングルメント集中化**とよばれる．

2 つの系 $\mathcal{H}_A, \mathcal{H}_B$ に跨った純粋状態 $|a\rangle$ と同一にある状態が n 個独立に与えられた場合のプロトコルを考える [3]．純粋状態 $|a\rangle$ の Schmidt 分解

$$|a\rangle = \sum_{j=1}^{r} \sqrt{p_j}|v_j\rangle \otimes |u_j\rangle \tag{6.46}$$

を用いて，プロトコルを与える．したがって，系 $\mathcal{H}_A, \mathcal{H}_B$ 上の縮約密度行列は $\sum_{j=1}^{r} p_j|v_j\rangle\langle v_j|, \sum_{j=1}^{r} p_j|u_j\rangle\langle u_j|$ となる．このとき，$\boldsymbol{n} \in \mathcal{T}_n^r$ に対して $\mathcal{H}_A$

と $\mathcal{H}_B$ への射影を Schmidt 基底 $\mathcal{B}_A := \{|v_j\rangle\}$, $\mathcal{B}_B := \{|u_j\rangle\}$ を用いて以下のように定義する．

$$P_{\boldsymbol{n}}^{\mathcal{B}_A} := \sum_{\vec{x}\in T_{\boldsymbol{n}}} |\vec{v}(\vec{x})\rangle\langle\vec{v}(\vec{x})|, \quad P_{\boldsymbol{n}}^{\mathcal{B}_B} := \sum_{\vec{x}\in T_{\boldsymbol{n}}} |\vec{u}(\vec{x})\rangle\langle\vec{u}(\vec{x})|.$$

すると，それぞれの系 $\mathcal{H}_A^{\otimes n}$, $\mathcal{H}_B^{\otimes n}$ 上の PVM $\{P_{\boldsymbol{n}}^{\mathcal{B}_A}\}_{\boldsymbol{n}}$, $\{P_{\boldsymbol{n}}^{\mathcal{B}_B}\}_{\boldsymbol{n}}$ が定義できる．合成系 $\mathcal{H}_A^{\otimes n}\otimes\mathcal{H}_B^{\otimes n}$ 上の純粋状態 $|a\rangle^{\otimes n}$ の系 $\mathcal{H}_A^{\otimes n}$, $\mathcal{H}_B^{\otimes n}$ 上の縮約密度行列は $\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r}\prod_{j=1}^r p_j^{n_j} P_{\boldsymbol{n}}^{\mathcal{B}_A}$, $\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r}\prod_{j=1}^r p_j^{n_j} P_{\boldsymbol{n}}^{\mathcal{B}_B}$ となる．したがって，合成系上の純粋状態 $|a\rangle^{\otimes n}$ は以下のように書ける．

$$|a\rangle^{\otimes n} = \sum_{\boldsymbol{n}\in\mathcal{Y}_n^r}\prod_{j=1}^r p_j^{n_j/2} \sum_{\vec{x}\in T_{\boldsymbol{n}}} |\vec{v}(\vec{x})\rangle\otimes|\vec{u}(\vec{x})\rangle.$$

このとき，それぞれの系で上の PVM $\{P_{\boldsymbol{n},A}\}_{\boldsymbol{n}}$, $\{P_{\boldsymbol{n},B}\}_{\boldsymbol{n}}$ に対応する測定を行うとする．それぞれの系での測定値が $\boldsymbol{n}$, $\boldsymbol{n}'$ となる確率は以下のように計算できる．

$$\begin{aligned}
&\|P_{\boldsymbol{n}}^{\mathcal{B}_A}\otimes P_{\boldsymbol{n}'}^{\mathcal{B}_B}|a\rangle^{\otimes n}\|^2 = \|(I\otimes P_{\boldsymbol{n}'}^{\mathcal{B}_B})(P_{\boldsymbol{n}}^{\mathcal{B}_A}\otimes I)|a\rangle^{\otimes n}\|^2 \\
&= \left\|(I\otimes P_{\boldsymbol{n}'}^{\mathcal{B}_B})(P_{\boldsymbol{n}}^{\mathcal{B}_A}\otimes I)\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r}\prod_{j=1}^r p_j^{n_j/2}\sum_{\vec{x}\in T_{\boldsymbol{n}}}|\vec{v}(\vec{x})\rangle\otimes|\vec{u}(\vec{x})\rangle\right\|^2 \\
&= \left\|(I\otimes P_{\boldsymbol{n}'}^{\mathcal{B}_B})\sum_{\boldsymbol{n}\in\mathcal{Y}_n^r}\prod_{j=1}^r p_j^{n_j/2}\sum_{\vec{x}\in T_{\boldsymbol{n}}}|\vec{v}(\vec{x})\rangle\otimes|\vec{u}(\vec{x})\rangle\right\|^2 \\
&= \delta_{\boldsymbol{n},\boldsymbol{n}'}\prod_{j=1}^r p_j^{n_j}|T_{\boldsymbol{n}}| = \delta_{\boldsymbol{n},\boldsymbol{n}'}\,\mathrm{Mul}[\boldsymbol{p},n](\boldsymbol{n}).
\end{aligned}$$

したがって，この2つの測定値は必ず一致する．また，このときの終状態は $\frac{1}{\sqrt{|T_{\boldsymbol{n}}|}}\sum_{\vec{x}\in T_{\boldsymbol{n}}}|\vec{v}(\vec{x})\rangle\otimes|\vec{u}(\vec{x})\rangle$ となり，サイズが $\log|T_{\boldsymbol{n}}|$ の最大エンタングル状態ができる．このプロトコルの構成は，(6.46) での Schmidt 基底にのみ依存する．

しかし，その性能は Schmidt 係数 $\sqrt{p_j}$ に依存する．このプロトコルでの生成桁数の平均値は $\sum_{\boldsymbol{n}\in T_n^r}\mathrm{Mul}[\boldsymbol{p},n](\boldsymbol{n})\log C(\boldsymbol{n})$ となる．この値の漸近的な振る舞いは補題 6.1.4 の (6.10) で与えられる．すなわち，ほぼ $nH(\boldsymbol{p})$ の最大

エンタングル状態が生成される．この量は漸近的に生成される最大エンタングル状態の最適なサイズである．

6.5.2 縮約密度行列の基底が未知の場合

上記のプロトコルは，Schmidt 基底に依存する．一般には，Schmidt 基底の情報も事前に与えられていないことも多い．そのような状況では，Schmidt 基底にも依存しない，ユニバーサルなエンタングルメントの集中化プロトコルが望まれる．

以下では，2 つの系 $\mathcal{H}_A, \mathcal{H}_B$ に跨った純粋状態 $|X\rangle\rangle$ と同一にある状態が n 個独立に与えられた場合に，Schmidt 基底にも依存しないユニバーサルなエンタングルメントの集中化プロトコルを与える [85]．それぞれのテンソル積空間は以下のように分解できる．

$$\mathcal{H}_A^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r(A)}} \mathcal{W}_{\boldsymbol{n},A} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r(A)}} \mathcal{U}_{\boldsymbol{n},A} \otimes \mathcal{V}_{\boldsymbol{n},A}, \tag{6.47}$$

$$\mathcal{H}_B^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r(B)}} \mathcal{W}_{\boldsymbol{n},B} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r(B)}} \mathcal{U}_{\boldsymbol{n},B} \otimes \mathcal{V}_{\boldsymbol{n},B}. \tag{6.48}$$

簡単のため，X は可逆な行列であるとする．この条件から必然的に，2 つの系 $\mathcal{H}_A, \mathcal{H}_B$ の次元は一致する．したがって，r を $\mathcal{H}_A$ の次元とすると，$\boldsymbol{n} \in \mathcal{Y}_{\boldsymbol{n}}^r$ について，$\mathcal{U}_{\boldsymbol{n},A}$ と $\mathcal{U}_{\boldsymbol{n},B}$ は同型である．そのため $\mathcal{U}_{\boldsymbol{n},A}$ 上の行列 $\mathsf{f}_{\boldsymbol{n}}(X)$ を $\mathcal{U}_{\boldsymbol{n},A}$ から $\mathcal{U}_{\boldsymbol{n},B}$ への行列と見なすことができる．この事実を用いると，合成系上の純粋状態 $|X\rangle\rangle^{\otimes n}$ は以下のように書ける．

$$|X\rangle\rangle^{\otimes n} = \sum_{\boldsymbol{n} \in \mathcal{Y}_n^r} |\mathsf{f}_{\boldsymbol{n}}(X)\rangle\rangle \otimes |I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle. \tag{6.49}$$

X が可逆でない場合，$|X\rangle\rangle$ のそれぞれの系への縮約密度行列の値域を $\mathcal{K}_A$, $\mathcal{K}_B$ とすると，それぞれの値域のテンソル積空間は以下のように分解できる．

$$\mathcal{K}_A^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} \mathcal{W}'_{\boldsymbol{n},A} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} \mathcal{U}'_{\boldsymbol{n},A} \otimes \mathcal{V}_{\boldsymbol{n},A}, \tag{6.50}$$

$$\mathcal{H}_B^{\otimes n} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} \mathcal{W}'_{\boldsymbol{n},B} = \bigoplus_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} \mathcal{U}'_{\boldsymbol{n},B} \otimes \mathcal{V}_{\boldsymbol{n},B}. \tag{6.51}$$

ここで，r' は X の縮約密度行列のランクである．このとき，合成系上の純粋状態 $|X\rangle\rangle^{\otimes n}$ は以下のように書ける．

$$|X\rangle\rangle^{\otimes n} = \sum_{\boldsymbol{n} \in \mathcal{Y}_n^{r'}} |\mathsf{f}_{\boldsymbol{n}}(X)\rangle\rangle \otimes |I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle. \tag{6.52}$$

$\mathcal{U}'_{\boldsymbol{n},A}, \mathcal{U}'_{\boldsymbol{n},B}$ は $\mathcal{U}_{\boldsymbol{n},A}, \mathcal{U}_{\boldsymbol{n},B}$ の部分空間であるので，$\mathcal{U}'_{\boldsymbol{n},A}$ から $\mathcal{U}'_{\boldsymbol{n},B}$ への行列 $\mathsf{f}_{\boldsymbol{n}}(X)$ は $\mathcal{U}_{\boldsymbol{n},A}$ から $\mathcal{U}_{\boldsymbol{n},B}$ への行列 $\mathsf{f}_{\boldsymbol{n}}(X)$ と見なすことができる．このように見なすと，$|\mathsf{f}_{\boldsymbol{n}}(X)\rangle\rangle \otimes |I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle$ は $\mathcal{U}_{\boldsymbol{n},A} \otimes \mathcal{U}_{\boldsymbol{n},B} \otimes \mathcal{V}_{\boldsymbol{n},A} \otimes \mathcal{V}_{\boldsymbol{n},B}$ 上の状態と見なせる．

以下，$\mathcal{W}_{\boldsymbol{n},A}$, $\mathcal{W}_{\boldsymbol{n},B}$ への射影を $P_{\boldsymbol{n},A}$, $P_{\boldsymbol{n},B}$ とする．それぞれの系 $\mathcal{H}_A^{\otimes n}$, $\mathcal{H}_B^{\otimes n}$ で測定 $\{P_{\boldsymbol{n},A}\}_{\boldsymbol{n}}$, $\{P_{\boldsymbol{n},B}\}_{\boldsymbol{n}}$ を行うと，その測定値が $\boldsymbol{n}$, $\boldsymbol{n}'$ となる確率は以下のように計算できる．

$$\begin{aligned}
\|P_{\boldsymbol{n},A} \otimes P_{\boldsymbol{n}',B}|A\rangle\rangle^{\otimes n}\|^2 &= \|(I \otimes P_{\boldsymbol{n}',B})(P_{\boldsymbol{n},A} \otimes I)|A\rangle\rangle^{\otimes n}\|^2 \\
&= \|(I \otimes P_{\boldsymbol{n}',B})(P_{\boldsymbol{n},A} \otimes I) \sum_{\boldsymbol{n} \in \mathcal{Y}_n^r} |\mathsf{f}_{\boldsymbol{n}}(A)\rangle\rangle \otimes |I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle\|^2 \\
&= \|(I \otimes P_{\boldsymbol{n}',B})|\mathsf{f}_{\boldsymbol{n}}(A)\rangle\rangle \otimes |I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle\|^2 = \delta_{\boldsymbol{n},\boldsymbol{n}'} Q[\rho^{\otimes n}](\boldsymbol{n}).
\end{aligned}$$

ここで，ρ を $\mathcal{H}_A$ での $|A\rangle\rangle$ の縮約密度行列とした．したがって，この2つの測定値は必ず一致する．また，このときの終状態は $\frac{1}{\sqrt{Q[\rho^{\otimes n}](\boldsymbol{n})}}|\mathsf{f}_{\boldsymbol{n}}(A)\rangle\rangle \otimes |I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle$ となる．この状態は系 $\mathcal{U}_{\boldsymbol{n},A} \otimes \mathcal{U}_{\boldsymbol{n},B} \otimes \mathcal{V}_{\boldsymbol{n},A} \otimes \mathcal{V}_{\boldsymbol{n},B}$ 上の状態である．ここで，系 $\mathcal{U}_{\boldsymbol{n},A} \otimes \mathcal{U}_{\boldsymbol{n},B}$ について部分トレースをとると，終状態は $\frac{1}{\sqrt{\dim \mathcal{W}_{\boldsymbol{n}}}}|I_{\mathcal{V}_{\boldsymbol{n}}}\rangle\rangle$ となる．すなわち，サイズが $\log \dim \mathcal{W}_{\boldsymbol{n}}$ の最大エンタングル状態ができる．このプロトコルでの生成サイズの平均値は $\sum_{\boldsymbol{n} \in \mathcal{Y}_n^r} Q[\rho^{\otimes n}](\boldsymbol{n}) \log \dim \mathcal{W}_{\boldsymbol{n}}$ となる．この値の漸近的な振る舞いは (6.31) で与えられる．この値は 6.5.2 項で与えた Schmidt 基底が既知である場合のプロトコルの平均性能 $\sum_{\boldsymbol{n} \in \mathcal{T}_n^r} \mathrm{Mul}[\boldsymbol{p}, n](\boldsymbol{n}) \log C(\boldsymbol{n})$ よりも小さい．(6.10) より，その差の極限値は

$$\frac{\sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \prod_i p_i^{\delta_{\sigma(i)}} \log \prod_j p_j^{\delta_{\sigma(j)}}}{\prod_{i,j:i<j}(p_i - p_j)} - \log \prod_{i,j:i<j} (p_i - p_j)$$

となる．このように，Schmidt 基底についての情報の有無で生成される最大エンタングル状態のサイズにはほとんど無視できる程度の差しか生じない．

6.6 量子情報源符号化

情報源符号化には，固定長型と可変長型がある．古典系の場合，固定長型は入力データに依存せずに圧縮率を決める方法であり，可変長型は入力データの冗長度に応じて圧縮率を決める方法である．そのため，固定長型はでは元のデータを完全に復号できないことが起き得る．しかし，情報源が従う確率分布に応じて適切な圧縮率の下，適切な圧縮方法を用いると，誤って復号される確率は小さくなる．一方，可変長型は適切な符号化・復号化を行うと，必ず元のデータを完全に復号できる．しかし，データに応じて，圧縮率が極めて悪くなることもある．場合によっては，元のデータよりも長くなることもある．しかし，情報源が従う確率分布に応じて適切な圧縮率の下，適切な圧縮方法を用いると，平均的な圧縮率を十分小さくすることができる．このように，固定長型では圧縮率は固定であり，復号の成否が確率変数となる．一方，可変長型は復号に必ず成功するが，圧縮率が確率変数となる．一般には，復号の成功が絶対条件であり，その上で圧縮率を減らすという需要があるので，現在のコンピュータで使われる情報源符号化は可変長型である．

6.6.1 固定長情報源符号化

量子系でのユニバーサルな固定長情報源符号化のプロトコルを与える [73, 41]．量子系での固定長情報源符号化の符号化プロセスは入力系となる量子系 $\mathcal{H}$ からメモリとなる量子系 $\mathcal{K}$ へのトレースを保存する完全正写像 E で与えられ，復号化プロセスはメモリとなる量子系 $\mathcal{K}$ から入力系となる量子系 $\mathcal{H}$ へのトレースを保存する完全正写像 D で与えられる．情報源は入力系 $\mathcal{H}$ 上の純粋状態についての確率分布 $\{\mathrm{P}(i), |x_j\rangle\langle x_j|\}$ を用いて与えられる．このとき，符号の性能は

$$\varepsilon_{\mathrm{P}}(E,D) := \sum_j \mathrm{P}(j)(1 - \langle x_j|D \circ E(|x_j\rangle\langle x_j|)|x_j\rangle) \tag{6.53}$$

を用いて表される．したがって，$\varepsilon_{\mathrm{P}}(E,D)$ と $\dim \mathcal{K}$ のトレードオフが問題となる．一般に，$\rho_{\mathrm{P}} := \sum_j \mathrm{P}(j)|x_j\rangle\langle x_j|$ とすると，(2.42) より，エンタングルメント忠実度を用いて，$\varepsilon_{\mathrm{P}}(E,D) \le 1 - F_e^2(D \circ E, \rho_{\mathrm{P}})$ と評価できる．すなわち，情報源のアンサンブルの形に依存せず，**平均密度行列** ρ_{P} にのみ依存した評価が可能となる．

次に，$\mathcal{K}$ から $\mathcal{H}$ への等長埋め込み写像 U に基づいて，符号化 E_U，復号化 D_U を以下のように定義する．

$$E_U(\rho) := U^\dagger \rho U + (\mathrm{Tr}\,\rho(I - U^\dagger U))\rho_{\mathrm{mix},\mathcal{K}}, \quad D_U(\rho) := U\rho U^\dagger. \tag{6.54}$$

このとき，$P_U := UU^\dagger$ とすると，$D_U \circ E_U(\rho) = P_U \rho P_U + (\mathrm{Tr}\,\rho(I - P_U))U\rho_{\mathrm{mix},\mathcal{K}}U^\dagger \le \Lambda[P_U](\rho)$ となる．したがって，$|X\rangle\rangle$ を ρ の純粋状態化とすると，$\langle\langle X|P_U \otimes I|X\rangle\rangle = \mathrm{Tr}\,\rho_{\mathrm{P}} P_U$ であるから，

$$\begin{aligned}
1 - F_e^2(D_U \circ E_U, \rho_{\mathrm{P}}) &\le 1 - F_e^2(\Lambda[P_U], \rho_{\mathrm{P}}) \\
&= 1 - \langle\langle X|P_U \otimes I|X\rangle\rangle\langle\langle X|P_U \otimes I|X\rangle\rangle = 1 - (\mathrm{Tr}\,\rho_{\mathrm{P}} P_U)^2 \\
&= 2(1 - \mathrm{Tr}\,\rho_{\mathrm{P}} P_U) - (1 - \mathrm{Tr}\,\rho_{\mathrm{P}} P_U)^2 \le 2\,\mathrm{Tr}\,\rho_{\mathrm{P}}(I - P_U)
\end{aligned}$$

を得る．上記のタイプの符号化・復号化に限って議論すると，U の値域への射影を P とすると，エラーの上限 $\mathrm{Tr}\,\rho_{\mathrm{P}}(I-P)$ とメモリの次元 $\mathrm{Tr}\,P$ の双方を小さくするトレードオフを扱う問題と見なすことができる．

次に，情報源が P の n 次の独立同一分布 P^n に従う場合を考える．このとき，入力系 $\mathcal{H}^{\otimes n}$ 上の平均密度行列は $\rho_{\mathrm{P}}^{\otimes n}$ で与えられる．$R > 0$ に対して，$Q[R,n] := \sum_{\boldsymbol{n}:H(\frac{\boldsymbol{n}}{n})\le R} P_{\boldsymbol{n}}$ とすると，(6.14), (6.16), (6.19) より，$\boldsymbol{p}$ を ρ_{P} の固有値からなるベクトルとすると，

$$\begin{aligned}
&\mathrm{Tr}\,Q[R,n] \le (n+1)^{r-1}e^{nR}, \quad \mathrm{Tr}\,\rho_{\mathrm{P}}^{\otimes n}Q[R,n] \\
&\le \max_{\boldsymbol{q}:H(\boldsymbol{q})\le R}(n+1)^{r(r+1)/2}e^{-nD(\boldsymbol{q}\|\boldsymbol{p})}
\end{aligned} \tag{6.55}$$

を得る．$Q[R,n]$ の値域を $\mathcal{K}_n$ とし，$\mathcal{K}_n$ から $\mathcal{H}^{\otimes n}$ への埋め込み等長写像を U_n とすると，符号化 E_{U_n}，復号化 D_{U_n} は以下を満たす．

$$\lim_{n\to\infty}\frac{-1}{n}\log \varepsilon_{\mathrm{P}}(E_{U_n}, D_{U_n}) = \min_{\boldsymbol{q}:H(\boldsymbol{q})\le R} D(\boldsymbol{q}\|\boldsymbol{p}), \tag{6.56}$$

$$\lim_{n\to\infty}\frac{-1}{n}\log\dim\mathcal{K}_n = R. \tag{6.57}$$

すなわち，$H(\boldsymbol{p}) = H(\rho) > R$ のとき，(6.56) の値は正の値となり，$\varepsilon_{\mathrm{P}}(E_{U_n}, D_{U_n})$ は指数的に減少する．この事実は，条件 $H(\rho) > R$ さえ満たされれば，情報源の形に依存せずに，漸近的にエラーが 0 となる固定長の情報源符号化が可能であることを示している．

6.6.2　可変長情報源符号化 I：圧縮率確定型

6.6.1 項の議論から，情報源のエントロピーレート $H(\rho_{\mathrm{P}})$ の情報さえ既知であれば，エントロピーレートを達成する符号が構成できることがわかる．しかし，情報源のエントロピーレート $H(\rho_{\mathrm{P}})$ さえわからない状況では，6.6.1 項で与えた固定長情報源符号化プロトコルは使えない．このような場合には，可変長情報源符号化が必要となる．

古典系での可変長符号化では圧縮率が入力データに依存して決まる．量子版の可変長情報源符号化では，入力系の量子状態に応じてメモリのサイズが決まることになる．このとき，量子状態を保存する量子メモリのサイズを確定させるためには，測定が必要となる．このようなタイプの情報源圧縮を圧縮率確定型の量子可変長情報源符号化とよぶ．一般に測定により状態は破壊されるので，圧縮率確定型では古典系のときのように完全に量子状態が復元できるというわけではない．むしろ，測定により状態破壊が生じ，一部の情報が失われる．6.6.1 項の議論より，エントロピーレート $H(\rho_{\mathrm{P}})$ さえわかれば，情報の圧縮は可能であるので，エントロピーレート $H(\rho_{\mathrm{P}})$ の推定と状態破壊の間のトレードオフを扱うことになる．

したがって，符号化プロセスは圧縮率とそれに応じた状態変化の双方の情報を持つ，Instrument $\{\Lambda_\omega\}_\omega$ によって与えられる．ここで，測定値 ω に対して，圧縮率を $R(\omega)$ に定めるとする．そして，圧縮率 $R(\omega)$ に応じて，復号化となる量子通信路 D_ω を決める．このようなプロトコルを $\Phi = (\{\Lambda_\omega\}_\omega, \{R(\omega)\}_\omega, \{D_\omega\})$ と記す．情報源が入力系 $\mathcal{H}$ 上の純粋状態についての確率分布 $\{\mathrm{P}(i), |x_j\rangle\langle x_j|\}$ を用いて与えられるとき，符号の性能は確率分布 $\sum_i \mathrm{P}(i)\,\mathrm{Tr}\,\Lambda_\omega(|x_i\rangle\langle x_i|)$ の下での確率変数 $R(\omega)$ の振る舞いと，初期状態と忠実度の二乗の期待値 $F^2(\{\Lambda_\omega\}_\omega, \{D_\omega\}) := \sum_i \mathrm{P}(i) \sum_\omega \mathrm{Tr}\,\Lambda_\omega(|x_j\rangle\langle x_j|) \langle x_j| \frac{D_\omega(\Lambda_\omega(|x_j\rangle\langle x_j|))}{\Lambda_\omega(|x_j\rangle\langle x_j|)} |x_j\rangle = \sum_i \mathrm{P}(i) \sum_\omega \langle x_j| D_\omega(\Lambda_\omega(|x_j\rangle\langle x_j|))|x_j\rangle$ を用いて表すことができる．以下，Instrument $\{\Lambda_\omega\}_\omega$ が POVM $\{M_\omega\}_\omega$ を用いて，$\Lambda_\omega(\rho) = \sqrt{M_\omega}\rho\sqrt{M_\omega}$ となり，メモリの空間が M_ω の値域であり，D_ω が恒等写像である場合を扱う．入力系が $\mathcal{H}$ で与えられるとき，$R(\omega)$ は $\frac{\log \mathrm{rank}\, M_\omega}{\log \dim \mathcal{H}}$ となり，

$$F^2(\{\Lambda_\omega\}_\omega, \{D_\omega\}) = \sum_i \mathrm{P}(i) \sum_\omega \langle x_i|\sqrt{M_\omega}|x_i\rangle\langle x_i|\sqrt{M_\omega}|x_i\rangle$$

$$= \sum_i \mathrm{P}(i) \sum_\omega \langle x_i | \sqrt{M_\omega} | x_i \rangle^2 \tag{6.58}$$

を得る．

ここで，入力系が $\mathbb{C}^{\otimes n}$ であり，入力系の情報源が $\mathbb{C}$ 上の純粋状態に関する分布 P の n 次の独立同一分布 P^n で与えられる場合を考える．M_ω として，$P_{\boldsymbol{n}}$ を用いると，圧縮率は漸近的に，エントロピーレート $H(\rho_{\mathrm{P}})$ に確率収束する．しかし，の二乗の期待値は 1 に収束せず，漸近的にもエラーが残る状況となる．このために，漸近的に状態の破壊がほとんどなく，漸近的に確率 1 でエントロピーレート $H(\rho_{\mathrm{P}})$ が推定できる測定を導入する．

実数 $\epsilon > 0$ に依存する行列 $M_{x,\epsilon}$ を，$U_{x,\epsilon} := (x-\epsilon, x+\epsilon]$ を用いて，以下のように定義する．$M_{x,\epsilon} := \sum_{\boldsymbol{n}:H(\frac{\boldsymbol{n}}{n}) \in U_{x,\epsilon}} P_{\boldsymbol{n}}$. すると，$\sum_{j\in\mathbb{Z}} M_{\epsilon j,\epsilon} = I$ となる．したがって，自然数 l について，$\sum_{j\in\mathbb{Z}} M_{\epsilon j,\epsilon l} = lI$ となる．$M_{\epsilon j}^{\epsilon,l} := \frac{1}{l} M_{\epsilon j,\epsilon l}$ とすると，$\{M_{\epsilon j}^{\epsilon,l}\}_{j\in\mathbb{Z}}$ は POVM となる．このとき，$\sqrt{M_{\epsilon j}^{\epsilon,l}} = \frac{1}{\sqrt{l}} M_{\epsilon j,\epsilon l}$ であるから，Jensen の不等式 (補題 2.3.6) を用いると，(6.58) の値は以下のように評価できる．

$$\begin{aligned}
\sum_{\boldsymbol{i}} \mathrm{P}^n(\boldsymbol{i}) \sum_{j\in\mathbb{Z}} \langle \boldsymbol{x_i} | \sqrt{M_{\epsilon j}^{\epsilon,l}} | \boldsymbol{x_i} \rangle^2 &= \sum_{\boldsymbol{i}} \mathrm{P}^n(\boldsymbol{i}) \sum_{j\in\mathbb{Z}} \frac{1}{l} \langle \boldsymbol{x_i} | M_{\epsilon j,\epsilon l} | \boldsymbol{x_i} \rangle^2 \\
\geq \sum_{j\in\mathbb{Z}} \frac{1}{l} \left(\sum_{\boldsymbol{i}} \mathrm{P}^n(\boldsymbol{i}) \langle \boldsymbol{x_i} | M_{\epsilon j,\epsilon l} | \boldsymbol{x_i} \rangle \right)^2 &= \sum_{j\in\mathbb{Z}} \frac{1}{l} (\mathrm{Tr}\, \rho_{\mathrm{P}}^{\otimes n} M_{\epsilon j,\epsilon l})^2.
\end{aligned} \tag{6.59}$$

$\epsilon j \in U_{H(\rho_{\mathrm{P}}),\epsilon(l-1)}$ となる $j \in \mathbb{Z}$ について，$U_{H(\rho_{\mathrm{P}}),\epsilon} \subset U_{\epsilon j,\epsilon l}$ が成り立つ．

$$\mathrm{Tr}\, \rho_{\mathrm{P}}^{\otimes n} M_{\epsilon j,\epsilon l} \geq \sum_{H(\frac{\boldsymbol{n}}{n}):U_{H(\rho_{\mathrm{P}}),\epsilon}} \mathrm{Tr}\, \rho_{\mathrm{P}}^{\otimes n} P_{\boldsymbol{n}} \tag{6.60}$$

を得る．$\epsilon j \in U_{H(\rho_{\mathrm{P}}),\epsilon(l-1)}$ を満たす $j \in \mathbb{Z}$ の数は $l-1$ 個なので，

$$\sum_{j\in\mathbb{Z}} \frac{1}{l} (\mathrm{Tr}\, \rho_{\mathrm{P}}^{\otimes n} M_{\epsilon j,\epsilon l})^2 \geq \frac{l-1}{l} \left(\sum_{H(\frac{\boldsymbol{n}}{n}):U_{H(\rho_{\mathrm{P}}),\epsilon}} \mathrm{Tr}\, \rho_{\mathrm{P}}^{\otimes n} P_{\boldsymbol{n}} \right)^2 \tag{6.61}$$

を得る．6.2.4 項の最初の議論から，ϵ_n が $\sqrt{n}\epsilon_n \to \infty$ を満たすとき，$\sum_{H(\frac{\boldsymbol{n}}{n}):U_{H(\rho_{\mathrm{P}}),\epsilon_n}} \mathrm{Tr}\, \rho_{\mathrm{P}}^{\otimes n} P_{\boldsymbol{n}}$ は 1 に収束する．ここで，ϵ を ϵ_n として選び，

l を $l_n \to \infty$, $\epsilon_n l_n \to 0$ を満たす l_n として選ぶと，(6.61) は 1 に収束する．すなわち，(6.59) より，(6.58) で与えた初期状態との二乗の期待値は 1 に収束する．

また，(6.14) と 6.2.4 項の最初の議論から，$n \to \infty$ の極限において，$\frac{1}{n}\log M^{\epsilon_n,l_n}_{\epsilon_n j}$ は漸近的に $\epsilon_n j$ に一致する．すなわち，$\max_{j\in\mathbb{Z}}|\frac{1}{n}\log M^{\epsilon_n,l_n}_{\epsilon_n j} - \epsilon_n j|$ は 0 に収束する．状態が $\rho_{\mathrm{P}}^{\otimes n}$ であるときに測定 $\{\mathrm{P}_{\boldsymbol{n}}\}$ を行った場合，$H(\frac{\boldsymbol{n}}{n})$ が $H(\rho_{\mathrm{P}})$ に確率収束することに注意すると，条件 $\epsilon_n l_n \to 0$ より，測定値 $\epsilon_n j$ は $H(\rho_{\mathrm{P}})$ に確率収束する．したがって，$\frac{1}{n}\log M^{\epsilon_n,l_n}_{\epsilon_n j}$ は $H(\rho_{\mathrm{P}})$ に確率収束する．このようにして，圧縮率確定型のユニバーサルな可変長情報源符号化が構成できる [43, 44].

6.6.3　古典系での語頭符号と Kraft の不等式

先に与えた量子系での可変長情報源符号化は漸近的には歪みが 0 に収束するものの，有限サイズでは，歪みが存在する．しかし，古典系では，歪みのない可変長情報源符号化が構成可能となる．情報源を表す集合が $\{1,\dots,d\}$ である場合，**無歪可変長符号**は，$\{1,\dots,d\}$ から $\{0,1\}^* := \bigcup_{n\ge 0}\{0,1\}^n$ への単射となる写像 ϕ で与えられる．そして，任意の $i\in\{1,\dots,d\}$ に対して，$\phi(i)$ を**符号語**といい，$\phi(i)\in\{0,1\}^n$ となる n を符号長といい，$|\phi(i)|$ と記す．例えば，情報源が確率分布 P に従う場合，**平均符号長**は $\sum_{i=1}^d \mathrm{P}(i)|\phi(i)|$ で与えられる．そして，$\{1,\dots,d\}$ 上の無歪可変長符号 ϕ は $l_i := |\phi(i)|$ とすると，以下の不等式を満たす．

$$\sum_{i=1}^d \frac{1}{2^{l_i}} \le \lceil \log_2 d \rceil. \tag{6.62}$$

(6.62) の証明.　$f(M)$ を $\{0,1\}^*$ から互いに異なる M 個の符号語 $\phi(1),\dots,\phi(M)$ を選んだときの値 $\sum_{i=1}^M 2^{-|\phi(i)|}$ の最大値を表すとする．$M = 2^1 + 2^2 + \cdots + 2^m$ のとき，$f(2^1+2^2+\cdots+2^m) = m$ となる．したがって，$f(d) \le f(2^1+2^2+\cdots+2^{\lceil\log_2 d\rceil}) \le \lceil\log_2 d\rceil$ となり題意を得る．□

しかし，2 つの無歪可変長符号 ϕ_1, ϕ_2 を結び付けると，$\{1,\dots,d\}^2$ から $\bigcup_{n\ge 0}\{0,1\}^n$ への単射となる写像 $\phi_1\cdot\phi_2$ が $\phi_1\cdot\phi_2(i,j) := \phi_1(i)\phi_2(j)$ で定義

できる．しかし，ϕ_1, ϕ_2 がともに単射であっても $\phi_1 \cdot \phi_2$ が単射であるとは限らない．無歪可変長符号 ϕ について，任意の n について，$\phi^n := \overbrace{\phi \cdot \cdots \cdot \phi}^{n}$ が単射であるとき，ϕ は**一意復号可能**であるという．また，$\{1,\ldots,d\}$ 上の無歪可変長符号 ϕ と $i \in \{1,\ldots,d\}$ に対して，任意の整数 $j \le |\phi(i)|$ について，$\phi(i)$ の第 j 番目までの要素を並べたものを**語頭**という．したがって，$\phi(i) = 0111$ のとき，0, 01, 011 が符号語 $\phi(i)$ の語頭となる．無歪可変長符号 ϕ の任意の符号語が他の符号語の語頭とならないとき，ϕ を**語頭符号**という．2つの語頭符号 ϕ_1, ρ_2 を繋げた写像 $\phi_1 \cdot \rho_2$ は語頭符号の条件から $\{1,\ldots,d\}^2$ から $\bigcup_{n\ge 0}\{0,1\}^n$ への単射となり，無歪可変長符号となる．さらに，無歪可変長符号 $\phi_1 \cdot \rho_2$ は語頭符号となることも確認できる．この議論を繰り返すことにより，語頭符号 ϕ について，ϕ^n は語頭符号となり，ϕ が一意復号可能であることが確認できる．しかし，一意復号可能な無歪可変長符号であっても語頭符号とは限らない [72, 例 1.14]．$\{1,\ldots,d\}$ 上の語頭符号 ϕ は $l_i := |\phi(i)|$ とすると，以下の **Kraft の不等式**を満たす．

$$\sum_{i=1}^{d} \frac{1}{2^{l_i}} \le 1. \tag{6.63}$$

実は，語頭符号ではない一般の一意復号可能な無歪可変長符号 ϕ は $l_i := |\phi(i)|$ とすると，以下の **McMillian の不等式**を満たす [31, 定理 3.8]．

$$\sum_{i=1}^{d} \frac{1}{2^{l_i}} \le 1. \tag{6.64}$$

Kraft の不等式 (6.63) は，McMillian の不等式から導かれる．

(6.64) の証明.　符号 ϕ^n に注目すると，$(\sum_{i=1}^{d} \frac{1}{2^{l_i}})^n = \sum_{i=1}^{d^n} \frac{1}{2^{\phi^n(i)}}$ となる．符号 ϕ^n に (6.62) を適用すると，$\sum_{i=1}^{d^n} \frac{1}{2^{\phi^n(i)}} \le \lceil n \log_2 d \rceil$ を得る．すなわち，$n \log(\sum_{i=1}^{d} \frac{1}{2^{l_i}}) \le \log \lceil n \log_2 d \rceil$ となる．両辺を n で割り，極限 $n \to \infty$ を考えると，$\sum_{i=1}^{d} \frac{1}{2^{l_i}} \le 1$ を得る．□

逆に，(6.63) を満たす整数の組 $\{l_i\}$ に対して，$l_i := |\phi(i)|$ となる語頭符号 ϕ が存在する．この語頭符号 ϕ の構成については例えば [72, 1.4 節] を見よ．こ

のように，(6.63) の左辺で与えられる確率分布には，上記の Kraft の不等式の意味で対応する語頭符号が存在する．すなわち，任意の確率分布 P の下での平均符号長が $\sum_{i=1}^{d} \mathrm{P}(i) l_i$ となる語頭符号が存在する．さらに，一般の確率分布 Q に対しても，$l_i = \lceil -\log_2 \mathrm{Q}(i) \rceil$ は条件 (6.63) を満たすことから，任意の確率分布 P の下での平均符号長が $-\sum_{i=1}^{d} \mathrm{P}(i) \log_2 \mathrm{Q}(i) + 1$ 以下となる語頭符号が存在する．このように，誤差 1 の範囲で，語頭符号に対応する確率分布 Q と情報源に対応する確率分布 P を用いて，平均符号長は $-\sum_{i=1}^{d} \mathrm{P}(i) \log_2 \mathrm{Q}(i)$ で表される．この値は $D(\mathrm{P}\|\mathrm{Q}) \geq 0$ であることから，

$$-\sum_{i=1}^{d} \mathrm{P}(i) \log_2 \mathrm{Q}(i) = \frac{H(\mathrm{P}) + D(\mathrm{P}\|\mathrm{Q})}{\log 2} \geq \frac{H(\mathrm{P})}{\log 2} \tag{6.65}$$

となる．情報源を表す確率分布が P であるとき，等号成立条件から，P に対応する語頭符号を用いたときに，平均符号長の最小値 $\frac{H(\mathrm{P})}{\log 2}$ が得られることがわかる．

6.6.4 可変長情報源符号化 II：圧縮率不確定型

6.6.2 項では圧縮率確定型のユニバーサルな可変長情報源符号化を構成したが，歪みが漸近的に 0 になるものの，完全に 0 にはできなかった．符号長決定に伴う測定による状態破壊を微小にすることはできても，情報源に非可換性が存在する場合は，完全になくすことは原理的に不可能であることが Koashi-Imoto [78] により示されている．

そのため，6.6.3 項で扱った古典系での議論のように状態破壊を完全になくす情報源圧縮のためには，符号長を決定するプロセスをあきらめざるを得ない．そのような可変長符号化を与えるためには，異なる符号長の重ね合わせを考えるため，空間 $\mathcal{H}_\oplus := \bigoplus_{k=0}^{\infty} (\mathbb{C}^2)^{\otimes k}$ を考え，情報源のなす d 次元の量子系 $\mathcal{H}$ から $\mathcal{H}_\oplus$ への等長写像 U によって，量子無歪可変長符号を与える [47]．そして，$(\mathbb{C}^2)^{\otimes k}$ への射影を P_k とし，$H := \sum_{k=0}^{\infty} k P_k$ とすると，情報源を表す密度行列が ρ_{P} で与えられるとき，**平均符号長**は $\mathrm{Tr}\, \rho U^\dagger H U$ で与えられる．このように符号長が確定しない設定では，上記の k をメモリサイズと捉えるよりも，エネルギーと捉えた方が自然である．一般に平均エネルギーが小さくなるように情報を保存する方がよい．そのため，情報の保存のための平均エネルギーをなるだけ少なくする戦略を採用することとする．

そして，以下の不等式が成り立つ [47].

補題 6.6.1　d 次元の量子系 $\mathcal{H}$ 上の任意の量子無歪可変長符号 U は

$$\operatorname{Tr} U^\dagger 2^{-H} U \leq \lceil \log_2 d \rceil \tag{6.66}$$

を満たす．そして，$\mathcal{H}$ 上の密度行列 $\sigma(U) := \frac{1}{\operatorname{Tr} U^\dagger 2^{-H} U} U^\dagger 2^{-H} U$ は以下を満たす．

$$-\operatorname{Tr} \rho \log_2 \sigma(U) - \log \lceil \log_2 d \rceil \leq \operatorname{Tr} HU\rho U^\dagger, \forall \rho \in \mathcal{S}(\mathcal{H}). \tag{6.67}$$

証明.　$f(M) := \max_{\operatorname{rank} P = M} \operatorname{Tr} 2^{-H} P$ と定義すると，$\operatorname{Tr} U^\dagger 2^{-H} U = \operatorname{Tr} 2^{-H} UU^\dagger \leq f(d)$ を得る．(6.62) の証明と同じ議論より，$f(d) \leq \lceil \log_2 d \rceil$ を得る．したがって，(6.66) を得る．

さらに，関数 $x \mapsto \log x$ の作用素凹性より，$-\log_2 U^\dagger 2^{-H} U \leq U^\dagger H U$ となる．したがって，(6.66) より，(6.67) を得る．　□

古典系でも述べたように，2つの量子無歪可変長符号を繋げても，一般にには量子無歪可変長符号は定まらない．古典系では2つの無歪可変長符号を繋げた写像は定義できたが，2つの量子無歪可変長符号 U_1, U_2 に対して，それらを繋げた写像さえ定義することが容易ではない．量子無歪可変長符号 U に対して，以下を満たす古典系の一意復号可能な無歪可変長符号 ϕ と d 次元の量子系 $\mathcal{H}$ の基底 $\{e_1, \ldots, e_d\}$ が存在するとき，U を**一意復号可能**という．

$$U = \sum_{i=1}^{d} |\phi(i)\rangle\langle e_i|. \tag{6.68}$$

このとき，U を n 個繋げた量子無歪可変長符号 $U^{(n)}$ は以下で定義される．

$$U^{(n)} = \sum_{i_1=1}^{d} \cdots \sum_{i_n=1}^{d} |\phi(i_1) \cdots \phi(i_n)\rangle\langle e_{i_1} \cdots e_{i_n}|. \tag{6.69}$$

特に，ϕ が語頭符号であるとき，U を**量子語頭符号**とよぶ．

McMillian の不等式 (6.64) より，d 次元の量子系 $\mathcal{H}$ 上の一意復号可能な量子無歪可変長符号 U は

$$\operatorname{Tr} U^\dagger 2^{-H} U = \sum_{i=1}^{d} 2^{-|\phi(i)|} \leq 1 \tag{6.70}$$

を満たす．逆に，量子系 $\mathcal{H}$ 上の任意の密度行列 σ に対して，以下を満たす量子語頭符号 U が存在する．

$$U^\dagger HU \leq -\log\sigma + I. \tag{6.71}$$

(6.71) の証明の証明.　σ の対角化 $\sigma = \sum_{i=1}^d \mathrm{Q}(i)|e_i\rangle\langle e_i|$ を考える．$l_i = \lceil -\log_2 \mathrm{Q}(i)\rceil$ は条件 (6.63) を満たすことから，$l_i = \phi(i)$ となる古典系の語頭符号が存在する．量子語頭符号 U を (6.68) で定義すると，(6.71) を得る．□

このように，誤差 1 の範囲で，量子語頭符号に対応する密度行列 σ と情報源に対応する密度行列 ρ を用いて，平均符号長は $-\operatorname{Tr}\rho\log_2\sigma$ で表される．この値は $D(\rho\|\sigma) \geq 0$ であることから，

$$-\operatorname{Tr}\rho\log_2\sigma = \frac{H(\rho) + D(\rho\|\sigma)}{\log 2} \geq \frac{H(\rho)}{\log 2} \tag{6.72}$$

となる．情報源を表す密度行列が ρ であるとき，等号成立条件から，ρ に対応する語頭符号を用いたときに，平均符号長の最小値 $\frac{H(\rho)}{\log 2}$ が得られることがわかる．そのため，量子相対エントロピー $D(\rho\|\sigma)$ は**冗長度**と見なすことができる．

情報源を表す密度行列 ρ が未知であり，ρ の候補が複数考えられる場合，$D(\rho\|\sigma)$ を一様に小さくする σ を見つけるにはどのようにすればよいであろうか？　一般には候補となる ρ にまったく仮定がない場合はまれである．今，情報源の物理系を表す Hilbert 空間が $\mathcal{H} := \mathbb{C}^d$ のテンソル積空間 $\mathcal{H}^{\otimes n}$ で与えられ，情報源を表す密度行列がテンソル積状態 $\rho^{\otimes n}$ で与えられると仮定し，ρ のとり方に依存せず，冗長度 $D(\rho^{\otimes n}\|\sigma)$ を一様に小さくする σ を見つける問題を考える．これは，テンソル積状態 $\rho^{\otimes n}$ を量子相対エントロピーの意味で一様に近似する問題と見なすこともできる．6.4 節の議論より，適切に $\mathcal{H}^{\otimes n}$ 上の密度行列 σ_n を選ぶと，

$$D(\rho^{\otimes n}\|\sigma_n) \cong \frac{d^2-1}{2}\log n + C_{\min-\max}(d) \tag{6.73}$$

となる．このとき，d^2-1 は密度行列のなす空間の次元と一致するので，この議論は，古典系での結果と同じ結論である．より詳細な定数項についての最適化は定理 6.4.3 でなされている．

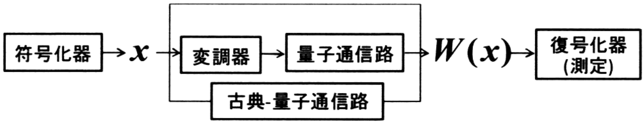


図 6.2　古典-量子通信路符号化

また，情報源がどのような n 次の独立同一分布 P に従う場合でも，情報源を記述する密度行列は $\rho_{\mathrm{P}}^{\otimes n}$ となる．したがって定理6.4.3で与えた密度行列 $\rho_{J,n}$ または $\tilde{\rho}_{J,n}$ を用いることで，ユニバーサルな量子無歪可変長符号が構成できる [47].

6.7　古典-量子通信路符号化

第5章ではノイズのある量子通信路を用いて量子状態を伝送する問題を扱ったが，本節ではノイズのある量子通信路を用いて古典情報を伝送する問題を扱う．伝送する情報を古典情報に限った方が解析が容易になるため，量子通信路に依存しないユニバーサルな符号化・復号化を扱う．この設定では，あらかじめ入力の量子系 $\mathcal{H}'$ から出力の量子系 $\mathcal{H}=\mathbb{C}^d$ への量子通信路 Λ と古典的なアルファベットの集合 $\mathcal{X}:=\{x_1,\ldots,x_k\}$ から入力の量子系 $\mathcal{H}'$ の状態集合 $\mathcal{S}(\mathcal{H})$ の写像 $x\mapsto\rho_x$ を固定する．すると，入力アルファベットが i であるとき，出力系での量子状態は $W(x):=\Lambda(\rho_x)$ となる．以下では，古典的なアルファベット x から出力系の量子状態 $W(x)$ を与える写像を**古典-量子通信路**とよぶことにする．一般に，古典-量子通信路が与えられれば，量子通信路を用いて，古典情報を伝送する問題を扱うことができる．伝送したいメッセージの集合が $\{1,\ldots,M\}$ であるとき，符号化は $\{1,\ldots,M\}$ から $\mathcal{X}$ への写像 ϕ で与えられる．そして，復号化はメッセージの集合 $\{1,\ldots,M\}$ に値を持つ POVM $\{Y_i\}_{i=1}^M$ を用いて与えられる．したがって，$(M,\phi,\{Y_i\}_{i=1}^M)$ を符号とよび，Φ と記す．符号 Φ の性能は伝送できるメッセージのサイズ $|\Phi|:=M$ と，平均誤り確率 $\varepsilon(\Phi):=1-\sum_{i=1}^M \mathrm{Tr}\,W(\phi(i))Y_i$ によって特徴付けられる．

以下では，同一の古典-量子通信路を n 回用いて古典的なメッセージを伝送する問題を扱う．そのため，以下ではアルファベット集合 $\mathcal{X}^n$ から $\mathcal{H}^{\otimes n}$ への古典-量子通信路 $W^{(n)}(\vec{x}):=W(x_1)\otimes\cdots\otimes W(x_n)$ を注目する．このとき，**量子伝送情報量** $I(p:W)$ を用いて，伝送可能なメッセージのレートが以下の

ように表せる（例えば，林 [36] の第 4 章を参照のこと）.

定理 6.7.1 (Holevo[63], Schumacher, Westmoreland [101]) 古典-量子通信路の系列 $\{W^{(n)}\}$ に対する符号の列 $\{\Phi_n\}$ について

$$C(W) := \sup_{\{\Phi_n\}} \{\limsup_{n\to\infty} \frac{1}{n} \log|\Phi_n| | \varepsilon(\Phi_n) \to 0\} = \max_p I(p : W) \tag{6.74}$$

が成り立つ.

特に，$C(W)$ は漸近的に平均誤り確率 0 で伝送可能なメッセージのレートを表す．残念ながら，古典-量子通信路 W に依存せずに，漸近的に平均誤り確率 0 でメッセージのレート $C(W)$ を実現することで符号を構成することはできない．しかしながら，漸近的に平均誤り確率 0 でメッセージのレート $I(p : W)$ であれば，古典-量子通信路 W に依存せずに達成できる．そのような符号の系列は古典-量子通信路に対するユニバーサル符号とよばれる．具体的には，任意の $\mathcal{X}$ 上の確率分布 $\boldsymbol{p}$ に対して以下を満たす符号の系列 $\{\Phi_n\}_{n=1}^{\infty}$ が存在する [48]．任意の古典-量子通信路 W に対して，$\phi_{W,\boldsymbol{p}}(t) := -(1-t)\log \mathrm{Tr}(\sum_{x=1}^{k} p_x W(x)^{1-t})^{\frac{1}{1-t}}$ を定義すると，

$$\lim_{n\to\infty} \frac{-1}{n} \log \varepsilon[\Phi_n, W] \geq \max_{0\leq t\leq 1} \frac{\phi_{W,\boldsymbol{p}}(t) - tR}{1+t} \tag{6.75}$$

$$\lim_{n\to\infty} \frac{1}{n} \log|\Phi_n| = R \tag{6.76}$$

が成り立つ．ここで，$\phi_{W,\boldsymbol{p}}(t)$ の微分は $\phi'_{W,\boldsymbol{p}}(0) = I(\boldsymbol{p}, W)$ であるので，伝送レート R が量子相互情報量 $I(\boldsymbol{p}, W)$ より小さいとき，$\phi_{W,\boldsymbol{p}}(t) - tR > 0$ を満たす $t \in (0,1)$ が存在するため，$\max_{0\leq t\leq 1} \frac{\phi_{W,\boldsymbol{p}}(t)-tR}{1+t} > 0$ となり，平均誤り確率は 0 に収束する.

6.7.1 符号の構成

以下，(6.75),(6.76) を満たすユニバーサル符号の構成のために，6.1 節で導入したタイプの概念を条件付き確率の場合に拡張する．$\mathcal{X} = \{x_1, \ldots, x_k\}$ に加え，有限個の要素からなる確率空間 $\mathcal{Z} := \{z_1, \ldots, z_l\}$ を考える．そして，$\mathcal{X}$ 上のタイプ $\boldsymbol{n} = (n_1, \ldots, n_k) \in \mathcal{T}_n(\mathcal{X})$ が与えられたとき，$\mathcal{Z}$ 上の k 個のタイ

プの組 $\boldsymbol{V} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k) \in \mathcal{T}_{n_1}(\mathcal{Z}) \times \cdots \times \mathcal{T}_{n_k}(\mathcal{Z})$ を $\boldsymbol{n} \in \mathcal{T}_n(\mathcal{X})$ に付随した条件付きタイプとよぶ．$\boldsymbol{n} \in \mathcal{T}_n(\mathcal{X})$ に付随した $\mathcal{Z}$ 上の条件付きタイプの集合を $V(\boldsymbol{n}, \mathcal{Z})$ と記す．特に，条件付きタイプ $\boldsymbol{V}$ は自然に $\mathcal{X} \times \mathcal{Z}$ 上のタイプと見なせる．$\vec{x} \in \mathcal{X}^n$ と $\boldsymbol{n}(\vec{x})$ に付随した $\mathcal{Z}$ 上の条件付きタイプ $\boldsymbol{V}$ に対して，また，$(\frac{\boldsymbol{v}_1}{n_1}, \ldots, \frac{\boldsymbol{v}_k}{n_k})$ は条件付き分布となり，$\frac{\boldsymbol{V}}{\boldsymbol{n}}$ と記す．$\boldsymbol{V} \in V(\boldsymbol{n}(\vec{x}), \mathcal{Z})$ に対し，V shell とよばれる集合 $T_{\boldsymbol{V}}(\vec{x}) := \{\vec{y} \in \mathcal{Z}^n | (x_1, y_1), \ldots, (x_n, y_n) \in T_{\boldsymbol{V}}\}$ を定義する．

符号化を構成するために，初めに以下の補題を準備する．

補題 6.7.2 (Packing 補題 [21])　任意の $\boldsymbol{p} \in \mathcal{T}_n(\mathcal{X})$ と $R < H(\boldsymbol{p})$ に対して，$M_n := e^{n(R - \frac{1}{\sqrt{n}})}$ とする．$T_{n\boldsymbol{p}}$ に属する M_n 個の以下を満たす $\mathcal{X}^n$ の要素 $\mathcal{M}_n := \{\vec{x}_1, \ldots, \vec{x}_{M_n}\}$ が存在する．

$$|T_{\boldsymbol{V}}(\vec{x}) \cap (\mathcal{M}_n \setminus \{\vec{x}\})| \le |T_{\boldsymbol{V}}(\vec{x})| e^{-n(H(\boldsymbol{p}) - R)},$$
$$\forall \vec{x} \in \mathcal{M}_n, \forall \boldsymbol{V} \in V(\boldsymbol{n}(\vec{x}), \mathcal{X}).$$

以下では，符号化 ϕ の像が上の補題で与えられる $\mathcal{M}_n$ になるように選ぶ．$\vec{x} \in \mathcal{X}^n$ に対して，置換群 S_n の部分群 $S_{\vec{x}} := \{g \in S_n \,|\, g(\vec{x}) = \vec{x}\}$ を定義する．$\vec{x}' \neq \vec{x} \in \mathcal{X}$ に対して，$\vec{x}' \in T_{\boldsymbol{V}}(\vec{x})$ となる $\boldsymbol{V} \in V(\boldsymbol{n}(\vec{x}), \mathcal{X})$ を選ぶ．このとき，$\frac{\boldsymbol{V}}{\boldsymbol{n}(\vec{x})}$ を記述する確率遷移行列が恒等行列にならない，すると，$\mathcal{M}_n$ 上の一様分布 $p_{\mathcal{M}_n}$ は補題 6.7.2 より，

$$\begin{aligned}\sum_{g \in S_{\vec{x}}} \frac{1}{|S_{\vec{x}}|} p_{\mathcal{M}_n} \circ g(\vec{x}') =& \frac{|T_{\boldsymbol{V}}(\vec{x}) \cap \mathcal{M}_n|}{|T_{\boldsymbol{V}}(\vec{x})|} \frac{1}{|\mathcal{M}_n|} = \frac{|T_{\boldsymbol{V}}(\vec{x}) \cap (\mathcal{M}_n \setminus \{\vec{x}\})|}{|T_{\boldsymbol{V}}(\vec{x})| \cdot |\mathcal{M}_n|} \\ \le& e^{-nH(\boldsymbol{p})} e^{\sqrt{n}} = \boldsymbol{p}^n(\vec{x}') e^{\sqrt{n}} \end{aligned} \tag{6.77}$$

を満たす．ここで，$g(\vec{x})$ は $T_{\boldsymbol{V}}(\vec{x})$ の要素を一様に動くことから最初の等式が得られる．$\vec{x}' \in T_{\boldsymbol{p}}$ は $e^{-nH(\boldsymbol{p})} = \boldsymbol{p}^n(\vec{x}')$ を満たすことから最後の等式が得られる．

次に，復号化となる POVM を構成するために，$\vec{x} \in \mathcal{X}^n$ に対して，$W^{(n)}(\vec{x})$ を一様に近似する $\rho_{\vec{x}}$ を構成する．簡単のために，$\vec{x}' = (\underbrace{1, \ldots, 1}_{m_1}, \underbrace{2, \ldots, 2}_{m_2}, \ldots, \underbrace{k, \ldots, k}_{m_k})$ となる場合について $\rho_{\vec{x}'} := \rho_{U,m_1} \otimes \rho_{U,m_2} \otimes \cdots \otimes \rho_{U,m_k}$ を定義す

る．一般の $\vec{x} \in \mathcal{X}^n$ に対しては，$\boldsymbol{n}(\vec{x}) = \boldsymbol{n}(\vec{x}')$ となる上記の $\vec{x}'$ について定義された $\rho_{\vec{x}'}$ のテンソルの順番を入れ替えたものとして定義する．すると，(6.36) より，$\rho_{\vec{x}}$ は $\rho_{U,n}$ と可換となる．さらに，(6.37) より，

$$(n+1)^{\frac{k(r+2)(r-1)}{2}} \rho_{\vec{x}} \geq W_n(\vec{x}) \tag{6.78}$$

を得る．そして，任意の実数 $C_n > 0$ に対して，射影 $P(\vec{x}) := \{\rho_{\vec{x}} - C_n \rho_{U,n} \geq 0\}$ を定義し，以下のように復号化を定義する．

$$Y_{\vec{x}'} := \sqrt{\sum_{\vec{x} \in \mathcal{M}_n} P(\vec{x})}^{-1} P(\vec{x}') \sqrt{\sum_{\vec{x} \in \mathcal{M}_n} P(\vec{x})}^{-1}.$$

ここで構成した符号 $\Phi_{U,n}(\boldsymbol{p}, R) := (e^{nR-\sqrt{n}}, \mathcal{M}_n, \{Y_{\vec{x}}\}_{\vec{x} \in \mathcal{M}_n})$ は古典-量子通信路 W に依存せず，入力アルファベット上の確率分布 p にのみ依存する．

6.7.2 性能評価

平均誤り確率の評価において重要な役割を果たす不等式を準備する [36, 第 4 章].

補題 6.7.3 $I \geq S \geq 0, T \geq 0$ となる 2 つのエルミート行列 S, T は不等式 $I - \sqrt{S+T}^{-1} S \sqrt{S+T}^{-1} \leq 2(I-S) + 4T$ を満たす．

この不等式を適用することで，

$$I - Y_{\vec{x}'} \leq 2(I - P(\vec{x}')) + 4 \sum_{\vec{x}(\neq \vec{x}') \in \mathcal{M}_n} P(\vec{x})$$

を得る．したがって，古典-量子通信路 $W^{(n)}$ の下での符号 $\Phi_{U,n}(\boldsymbol{p}, R)$ の平均誤り確率は以下のように評価できる．

$$\begin{aligned}
&\frac{1}{|\mathcal{M}_n|} \sum_{\vec{x}' \in \mathcal{M}_n} \operatorname{Tr} W^{(n)}(\vec{x}')(I - Y_{\vec{x}'}) \\
&\leq \frac{2}{|\mathcal{M}_n|} \sum_{\vec{x}' \in \mathcal{M}_n} \operatorname{Tr} W^{(n)}(\vec{x}')(I - P(\vec{x}')) + \frac{4}{|\mathcal{M}_n|} \sum_{\vec{x}' \in \mathcal{M}_n} \operatorname{Tr} W^{(n)}(\vec{x}') \sum_{\vec{x}(\neq \vec{x}') \in \mathcal{M}_n} P(\vec{x}) \\
&= \frac{2}{|\mathcal{M}_n|} \sum_{\vec{x} \in \mathcal{M}_n} \operatorname{Tr} W^{(n)}(\vec{x})(I - P(\vec{x}))
\end{aligned}$$

$$+4\,\mathrm{Tr}\left[\sum_{\vec{x}\in\mathcal{M}_n} P(\vec{x})\left(\frac{1}{|\mathcal{M}_n|}\sum_{\vec{x}'(\neq\vec{x})\in\mathcal{M}_n} W^{(n)}(\vec{x}')\right)\right]. \tag{6.79}$$

密度行列 $\rho_{\vec{x}}$ は密度行列 $\rho_{U,n}$ と可換であるので，$0 \le t \le 1$ について

$$(I - P(\vec{x})) = \{\rho_{\vec{x}} - C_n\rho_{U,n} < 0\} \le \rho_{\vec{x}}^{-t} C_n^t \rho_{U,n}^t \tag{6.80}$$

を得る．さらに，密度行列 $\rho_{\vec{x}}$ は密度行列 $W^{(n)}(\vec{x})$ とも可換であるので，$W^{(n)}(\vec{x})\rho_{\vec{x}}^{-t}$ はエルミート行列となる．さらに，(6.78) より，

$$W^{(n)}(\vec{x})\rho_{\vec{x}}^{-t} \le (n+1)^{\frac{kt(r+2)(r-1)}{2}} W^{(n)}(\vec{x})^{1-t} \tag{6.81}$$

を得る．不等式 (6.80), (6.81) より，

$$\begin{aligned}\mathrm{Tr}\,W^{(n)}(\vec{x})(I - P(\vec{x})) &\le \mathrm{Tr}\,W^{(n)}(\vec{x})\rho_{\vec{x}}^{-t}\rho_{U,n}^t C_n^t \\ &\le (n+1)^{\frac{kt(r+2)(r-1)}{2}} C_n^t\,\mathrm{Tr}\,W^{(n)}(\vec{x})^{1-t}\rho_{U,n}^t \end{aligned} \tag{6.82}$$

を得る．値 $\mathrm{Tr}\,W^{(n)}(\vec{x})(I - P(\vec{x}))$ は $\vec{x}$ に対して置換を施しても不変であることと，$C(\boldsymbol{n}) = T_{\boldsymbol{n}}$ に関する評価 (6.4) より，$\vec{x} \in T_{\boldsymbol{p}}$ について

$$\boldsymbol{p}^n(\vec{x}) = e^{-nH(\boldsymbol{p})} \ge \frac{(n+1)^{-r}}{|T_{n\boldsymbol{p}}|} \tag{6.83}$$

が成り立つ．よって，

$$\begin{aligned}\mathrm{Tr}\,W^{(n)}(\vec{x})(I - P(\vec{x})) &= \frac{1}{|T_{\boldsymbol{p}}|}\sum_{\vec{x}'\in T_{\boldsymbol{p}}} \mathrm{Tr}\,W^{(n)}(\vec{x}')(I - P(\vec{x}')) \\ &\le (n+1)^r \sum_{\vec{x}'\in\mathcal{X}^n} \boldsymbol{p}^n(\vec{x}')\,\mathrm{Tr}\,W^{(n)}(\vec{x}')(I - P(\vec{x}')) \qquad (6.84) \\ &\le (n+1)^{r+\frac{kt(r+2)(r-1)}{2}} C_n^t\,\mathrm{Tr}\left(\sum_{\vec{x}'\in\mathcal{X}^n} \boldsymbol{p}^n(\vec{x}')W^{(n)}(\vec{x}')^{1-t}\right)\rho_{U,n}^t \qquad (6.85) \\ &\le (n+1)^{r+\frac{kt(r+2)(r-1)}{2}} C_n^t \max_{\sigma}\mathrm{Tr}\left[\sum_{x\in\mathcal{X}} \boldsymbol{p}(x)W^{(n)}(x)^{1-t}\right]^{\otimes n}\sigma^t\end{aligned}$$

$$\leq (n+1)^{r+\frac{kt(r+2)(r-1)}{2}} C_n^t \left(\mathrm{Tr} \left(\left[\sum_{x \in \mathcal{X}} \boldsymbol{p}(x) W^{(n)}(x)^{1-t} \right]^{\otimes n} \right)^{\frac{1}{1-t}} \right)^{1-t} \tag{6.86}$$

$$= (n+1)^{r+\frac{kt(r+2)(r-1)}{2}} C_n^t \left(\mathrm{Tr} \left(\sum_{x \in \mathcal{X}} \boldsymbol{p}(x) W^{(n)}(x)^{1-t} \right)^{\frac{1}{1-t}} \right)^{n(1-t)}$$

$$= (n+1)^{r+\frac{kt(r+2)(r-1)}{2}} C_n^t e^{-n\phi_{W,\boldsymbol{p}}(t)} \tag{6.87}$$

を得る．ただし，不等式 (6.84), (6.85), (6.86) は，それぞれ，(6.83), (6.82), (2.24) から導かれる．

次に，(6.79) の第 2 項を群 $S_{\vec{x}}$ に関する不変性を用いて評価する．

$$\mathrm{Tr} \left[P(\vec{x}) \left(\frac{1}{|\mathcal{M}_n|} \sum_{\vec{x}'(\neq \vec{x}) \in \mathcal{M}_n} W^{(n)}(\vec{x}') \right) \right]$$

$$= \mathrm{Tr} \left[P(\vec{x}) \sum_{\vec{x}'(\neq \vec{x}) \in \mathcal{M}_n} p_{\mathcal{M}_n}(\vec{x}') W^{(n)}(\vec{x}') \right]$$

$$= \mathrm{Tr} \left[P(\vec{x}) \sum_{s \in S_{\vec{x}}} \frac{1}{|S_{\vec{x}}|} \sum_{\vec{x}'(\neq \vec{x}) \in \mathcal{M}_n} p_{\mathcal{M}_n}(\vec{x}') V_s W^{(n)}(\vec{x}') V_s^* \right]$$

$$= \mathrm{Tr} \left[P(\vec{x}) \sum_{\vec{x}'(\neq \vec{x}) \in \mathcal{M}_n} \sum_{s \in S_{\vec{x}}} \frac{1}{|S_{\vec{x}}|} p_{\mathcal{M}_n} \circ s^{-1}(\vec{x}') W^{(n)}(\vec{x}') \right]$$

$$\leq \mathrm{Tr} \left[P(\vec{x}) \sum_{\vec{x}'(\neq \vec{x}) \in \mathcal{M}_n} \boldsymbol{p}^n(\vec{x}') e^{\sqrt{n}} W^{(n)}(\vec{x}') \right] \tag{6.88}$$

$$= e^{\sqrt{n}} \mathrm{Tr} \left[P(\vec{x}) W_{\boldsymbol{p}}^{\otimes n} \right]$$

$$\leq e^{\sqrt{n}} \mathrm{Tr} \left[P(\vec{x}) (n+1)^{\frac{(r+2)(r-1)}{2}} \rho_{U,n} \right] \tag{6.89}$$

$$\leq e^{\sqrt{n}} \mathrm{Tr} \left[P(\vec{x}) (n+1)^{\frac{(r+2)(r-1)}{2}} C_n^{-1} \rho_{\vec{x}} \right] \tag{6.90}$$

$$\leq e^{\sqrt{n}} \operatorname{Tr}\left[(n+1)^{\frac{(r+2)(r-1)}{2}} C_n^{-1} \rho_{\vec{x}}\right] = e^{\sqrt{n}} (n+1)^{\frac{(r+2)(r-1)}{2}} C_n^{-1}. \qquad (6.91)$$

ここで，不等式 (6.88), (6.89), (6.90) はそれぞれ，(6.77), (6.37)，および不等式 $P(\vec{x})(\rho_{U,n} - C_n^{-1}\rho_{\vec{x}}) \leq 0$ から導かれる．

以下，任意の $t \in (0,1)$, $R > 0$ に対して，$M_n := e^{nR-\sqrt{n}}$, $C_n := e^{n(R+f(t))}$, $f(t) := \frac{\phi_{W,\boldsymbol{p}}(t)-tR}{1+t}$ を選ぶ．$f(t) = \phi_{W,\boldsymbol{p}}(t) - t(R+f(t))$ であるから，(6.79), (6.87), (6.91) より，平均誤り確率は以下のように評価できる．

$$\begin{aligned}&\varepsilon(\Phi_{U,n}(\boldsymbol{p}, R), W)\\ &\quad \leq 2(n+1)^{r+\frac{kt(r+2)(r-1)}{2}} e^{-n(\phi_{W,\boldsymbol{p}}(t)-t(R+f(t)))} + 4(n+1)^{\frac{(r+2)(r-1)}{2}} e^{-nf(t)}.\end{aligned} \qquad (6.92)$$

したがって，指数的な減少レートは以下のように特徴付けられる．

$$\lim_{n\to\infty} \frac{-1}{n} \log \varepsilon(\Phi_{U,n}(\boldsymbol{p}, R), W) \geq \min\{\phi_{W,\boldsymbol{p}}(t) - t(R+f(t)), f(t)\} = \frac{\phi_{W,\boldsymbol{p}}(t) - tR}{1+t}.$$

すなわち，$t_0 := \operatorname{argmax}_{t\in(0,1)} \frac{\phi_{W,\boldsymbol{p}}(t)-tR}{1+t}$, $|\mathcal{M}_n| := e^{nR-\sqrt{n}}$, $C_n := e^{n(R+f(t_0))}$ となるように選ぶと，

$$\lim_{n\to\infty} \frac{-1}{n} \log \varepsilon(\Phi_{U,n}(\boldsymbol{p}, R), W) \geq \max_{t\in(0,1)} \frac{\phi_{W,\boldsymbol{p}}(t) - tR}{1+t}$$

が任意の古典-量子通信路 W について成り立つ．

演習問題略解

演習問題 1

x_1, x_2 を f の定義域の任意の2つの要素とする．任意の $\lambda \in [0,1]$ について，f の線形性より，$f(\lambda x_1 (1-\lambda) x_2) = \lambda f(x_1) + (1-\lambda) f(x_2)$ となる．さらに，g が凸関数であることから，$g(\lambda f(x_1) + (1-\lambda) f(x_2)) \leq \lambda g(f(x_1)) + (1-\lambda) g(f(x_2))$ となる．これら2つの不等式を組み合わせることで，$g(f(\lambda x_1 (1-\lambda) x_2)) \leq \lambda g(f(x_1)) + (1-\lambda) g(f(x_2))$ となり題意を得る．

演習問題 2

行列 X について，$X = X_1 + X_2 i$ を満たす2つのエルミート行列 X_1, X_2 を選ぶ．すると，$|\operatorname{Tr} X\rho|^2 = (\operatorname{Tr} X_1\rho)^2 + (\operatorname{Tr} X_2\rho)^2$ が成り立つ．演習問題1より，$(\operatorname{Tr} X_1\rho)^2, (\operatorname{Tr} X_2\rho)^2$ は凸関数である．凸関数の和も凸関数であるから，題意を得る．

演習問題 3

$$
\begin{aligned}
I_\rho(A:B) &= H(\rho_A) + H(\rho_B) - H(\rho) \\
&= -\operatorname{Tr} \rho(\log \rho_A) \otimes I_B - \operatorname{Tr} \rho I_A \otimes (\log \rho_B) + \operatorname{Tr} \rho \log \rho \\
&= -\operatorname{Tr} \rho \log(\rho_A \otimes \rho_B) + \operatorname{Tr} \rho \log \rho = D(\rho \| \rho_A \otimes \rho_B).
\end{aligned}
$$

演習問題 4

固有値が λ となる固有ベクトル以外の固有ベクトルの間で巡回させた密度行列を考える．このような密度行列を等しい重みで平均をとって得られる密度行列の von Neumann エントロピーは $(1-\lambda)\log\dim\mathcal{H}+h(\lambda)$ に一致する．したがって，von Neumann エントロピーの凹性を用いると示せる．

演習問題 5

$\langle\Phi|F_m\otimes I|\Phi\rangle=\mathrm{Tr}\,F_m\rho$ であるから，以下を得る．

$$F_e^2(\rho,\Lambda)=\langle\Phi|(\Lambda\otimes id)(|\Phi\rangle\langle\Phi|)|\Phi\rangle \tag{6.93}$$

$$=\langle\Phi|\sum_m(F_m\otimes I)|\Phi\rangle\langle\Phi|(F_m\otimes I)^\dagger|\Phi\rangle \tag{6.94}$$

$$=\sum_m|\langle\Phi|F_m\otimes I|\Phi\rangle|^2=\sum_m|\,\mathrm{Tr}\,F_m\rho|^2. \tag{6.95}$$

参考文献

[1] Bagan, E., Baig, M. and Munoz-Tapia, R., "Quantum reverse-engineering and reference frame alignment without non-local correlations," *Phys. Rev. A*, **70**, 030301, 2004.

[2] Bagan, E., Ballester, M. A., Gill, R. D., Monras, A. and Munoz-Tapia, R., "Optimal full estimation of qubit mixed states," *Phys. Rev. A*, **73**, 032301, 2006.

[3] Bennett, C. H., Bernstein, H. J., Popescu, S. and Schumacher, B., "Concentrating Partial Entanglement by Local Operations," *Phys. Rev. A*, **53**, 2046, 1996.

[4] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 175–179, 1984.

[5] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. and Wootters, W. K., "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, **54**, 3824–3851, 1996.

[6] Bennett, C. H. and Wiesner, S. J., "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, **69**, 2881, 1992.

[7] Bhatia, R., *Matrix Analysis*, Springer-Verlag, New York, 1996.

[8] Bjelakovic, I., Deuschel, J.-D., Kruger, T., Seiler, R., Siegmund-Schultze R. and Szkola, A., "A quantum version of Sanov's theorem," *Comm. Math. Phys.*, **260**(3), 659–671, 2005.

[9] Bogomolov, N. A., "Minimax measurements in a general statistical decision theory," *Teor. Veroyatnost. i Primenen.*, **26**, 798–807, 1981. (English translation: *Theory Probab. Appl.*, **26**(4), 787–795, 1981.)

[10] Calderbank, A. R., Rains, E. M., Shor, P. W. and Sloane, N. J. A., "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, **78**, 405–408, 1997.

[11] Calderbank, A. R., Rains, E. M., Shor, P. W. and Sloane, N. J. A., "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, **44**, 1369–1387, 1998.

[12] Calderbank, A. R. and Shor, P. W., "Good quantum error correcting codes exist," *Phys. Rev. A*, **54**, 1098–1105, 1996.

[13] Carter, J. L. and Wegman, M. N., "Universal Classes of Hash Functions," *J. Comput. System Sci.*, **18**, 143–154, 1979.

[14] Cerf, N. J., Ipe, A. and Rottenberg, X., "Cloning of Continuous Quantum Variables," *Phys. Rev. Lett.*, **85**, 1754–1757, 2000.

[15] Choi, M.-D., "Completely Positive Linear Maps on Complex Matrices," *Lin. Alg. Appl.*, 285–290, 1975.

[16] Chiribella, G., D'Ariano, G. M. and Sacchi, M. F., "Optimal estimation of group transformations using entanglement," *Phys. Rev. A*, **72**, 042338, 2005.

[17] Chiribella, G., D'Ariano, G. M., Perinotti, P. and Sacchi, M. F., "Efficient use of quantum resources for the transmission of a reference frame," *Phys. Rev. Lett.*, **93**, 180503, 2004.

[18] Christandl, M., *The Structure of Bipartite Quantum States Insights from Group Theory and Cryptography*, PhD thesis, University of Cambridge, 2006.

[19] Collatz, L. and Sinogowitz, U., "Spektren endlicher Grafen," *Abh. Math. Sem. Univ. Hamburg*, **21**, 63–77, 1957.

[20] Cramer, H., *Mathematical methods of statistics*, Princeton University Press, 1946.

[21] Csiszár, I. and Körner, J., *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, 1981. (Cambridge University Press; 2nd edition, 2011.)

[22] Gallager, R. G., *Information Theory and Reliable Communication*, John Wiley & Sons, 1968.

[23] Gisin, N. and Massar, S., "Optimal Quantum Cloning Machines," *Phys. Rev. Lett.*, **79**, 2153, 1997.

[24] Gottesman, D., "Class of quantum error-correcting codes saturating the

quantum Hamming bound," *Phys. Rev. A*, **54**, 1862–1868, 1996.
[25] Gottesman, D., "Theory of fault-tolerant quantum computation," *Phys. Rev. A*, **57**, 127–137, 1998. (Preprint quant-ph/9702029.)
[26] Gottesman, D., "Fault-tolerant quantum computation with higher-dimensional systems," Preprint quant-ph/9802007v2, 1998.
[27] Grassl, M., Rotteler, M. and Beth, T., "Efficient Quantum Circuits for Non-Qubit Quantum Error-Correcting Codes", *Int. J. Found. Comput. Sci. (IJFCS)*, **14**(5), 757–775, 2003.
[28] Hamada, M., "Teleportation and entanglement distillation in the presence of correlation among bipartite mixed states," *Phys. Rev. A*, **68**, 012301, 2003.
[29] Hamada, M., "Notes on the Fidelity of Symplectic Quantum Error-Correcting Codes," *Int. J. Quant. Inf.*, **1**(4), 443–463, 2003.
[30] Hamada, M., "Reliability of Calderbank-Shor-Steane Codes and Security of Quantum Key Distribution," *J. Phys. A: Math. and Gen.*, **37**(34), 8303–8328, 2004.
[31] 韓太舜，小林欣吾，『情報と符号化の数理』，培風館，1999.
[32] Hashimoto, T., Hayashi, A., Hayashi, M. and Horibe, M., "Unitary-process discrimination with error margin," *Phys. Rev. A*, **81**, 062327, 2010.
[33] Harrow, A. W. and Nielsen, M. A., "How robust is a quantum gate in the presence of noise?" *Phys. Rev. A*, **68**, 012308, 2003.
[34] Hastings, M. B., "A Counterexample to Additivity of Minimum Output Entropy," *Nat. Phys.*, **5**, 255, 2009.
[35] Hayashi, A., Hashimoto, T. and Horibe, M., "Extended Quantum Color Coding," *Phys. Rev. A*, **71**, 012326, 2005.
[36] 林正人，『量子情報理論入門』，SGC ライブラリ **32**，サイエンス社，2004.
[37] 林正人，『量子論のための表現論』，共立出版，2014.
[38] Hayashi, M., *Quantum Information: An Introduction*, Springer, 2006.
[39] Hayashi, M., "Asymptotic estimation theory for a finite dimensional pure state model," *J. Phys. A: Math. and Gen.*, **31**, 4633–4655, 1998. (It is also appeared as Chapter 23 of *Asymptotic Theory of Quantum Statistical Inference*, M. Hayashi eds.)
[40] Hayashi, M., "Optimal sequence of POVMs in the sense of Stein's lemma in quantum hypothesis," *J. Phys. A: Math. and Gen.*, **35**, 10759–10773, 2002.
[41] Hayashi, M., "Exponents of quantum fixed-length pure state source coding," *Phys. Rev. A*, **66**, 032321, 2002.
[42] Hayashi, M. and Matsumoto, K., "Asymptotic performance of optimal state estimation in quantum two level system," quant-ph/0411073, 2004.

[43] Hayashi, M. and Matsumoto, K., "Quantum universal variable-length source coding," *Phys. Rev. A*, **66**, 022311, 2002.

[44] Hayashi, M. and Matsumoto, K., "Simple construction of quantum universal variable-length source coding," *Quant. Inf. Comput.*, **2**, Special Issue, 519–529, 2002; quant-ph/0209124, 2002.

[45] Hayashi, M., "Parallel Treatment of Estimation of SU(2) and Phase Estimation," *Phys. Lett. A*, **354**(3), 183–189, 2006.

[46] Hayashi, M., "Practical Evaluation of Security for Quantum Key Distribution," *Phys. Rev. A*, **74**, 022307, 2006.

[47] Hayashi, M., "Universal approximation of multi-copy states and universal quantum lossless data compression," *Comm. Math. Phys.*, **293**(1), 171–183, 2010.

[48] Hayashi, M., "Universal coding for classical-quantum channel" *Comm. Math. Phys.*, **289**(3), 1087–1098, 2009.

[49] Hayashi, M., "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Phys. Rev. A*, **76**, 012329, 2007.

[50] Hayashi, M., Markham, D., Murao, M., Owari, M. and Virmani, S., "Bounds on Multipartite Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication," *Phys. Rev. Lett.*, **96**, 040501, 2006.

[51] Hayashi, M., Markham, D., Murao, M., Owari, M. and Virmani, S., "The geometric measure of entanglement for a symmetric pure state with positive amplitudes," *J. Math. Phys.*, **50**, 122104, 2009.

[52] Hayashi, M., "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inform. Theory*, **57**, 3989–4001, 2011.

[53] Hayashi, M. and Tsurumaru, T., "Concise and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths," *New J. of Phys.*, **14**, 093014, 2012.

[54] Hayashi, M., "Fourier Analytic Approach to Quantum Estimation of Group Action," arXiv:1209.3463, 2012.

[55] Hayden, P. M., Horodecki, M. and Terhal, B. M., "The asymptotic entanglement cost of preparing a quantum state," *J. Phys. A: Math. and Gen.*, **34**, 6891–6898, 2001.

[56] Hein, M., Eisert, J. and Briegel, H. J., "Multi-party entanglement in graph states," *Phys. Rev. A*, **69**, 062311, 2004.

[57] Hein, M., Dür, W., Eisert, J., Raussendorf, R., Van den Nest, M. and Briegel, H.-J., "Quantum Computers, Algorithms and Chaos," edited by

G. Casati *et al.*, **115**, Varenna, Italy, 2005; quant-ph/0602096.

[58] Hiai, F., "Matrix Analysis: Matrix Monotone Functions, Matrix Means, and Majorization," *Interdiscip. Inform. Sci.*, **16**, 139–248, 2010.

[59] 日合文雄，柳研二郎，『ヒルベルト空間と線形作用素』，牧野書店，1995.

[60] Hiai, F. and Petz, D., "The proper formula for relative entropy and its asymptotics in quantum probability," *Commun. Math. Phys.*, **143**, 99–114, 1991.

[61] Hiroshima, T., "Majorization criterion for distillability of a bipartite quantum state," *Phys. Rev. Lett.*, **91**, 057902, 2003.

[62] Holevo, A. S., "Covariant measurements and uncertainty relations," *Rep. Math. Phys.*, **16**, 385–400, 1979.

[63] Holevo, A. S., "The capacity of the quantum channel with general signal states," *IEEE Trans. Inform. Theory*, **44**, 269, 1998; quant-ph/9611023, 1996.

[64] Holevo, A. S., *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, 1982; Originally published in Russian, 1980; 2nd Edition, Springer, 2012.

[65] Horodecki, P., "Separability criterion and inseparable mixed states with positive partial transposition," *Phys. Lett. A*, **232**, 333, 1997.

[66] Horodecki, M., and Horodecki, P., "Reduction criterion of separability and limits for a class of distillation protocols," *Phys. Rev. A.*, **59**, 4206, 1999.

[67] Horodecki, M., Horodecki, P. and Horodecki, R., "Separability of mixed states: necessary and sufficient conditions," *Phys. Lett. A*, **223**, 1–8, 1996.

[68] Zhu, H., Chen, L. and Hayashi, M., "Additivity and non-additivity of multipartite entanglement measures," *New J. Phys.*, **12**, 083002, 2010.

[69] Hübener, R., Kleinmann, M., Wei, T. C., González-Guillén, C. and Gühne, O., "The geometric measure of entanglement for symmetric states," *Phys. Rev. A*, **80**, 032324, 2009.

[70] 石坂智，小川朋宏，河内亮周，木村元，林正人，『量子情報科学入門』，共立出版，2012.

[71] Jamiolkowski, A., "Linear transformations which preserve trace and positive semidefiniteness of operators," *Rep. Math. Phys.*, **3**, 275, 1972.

[72] Jones, G. A. and Jones, J. M., *Information and Coding Theory*, Springer, 2000; 一樂重雄，河原正治，河原雅子 訳，『情報理論と符号理論』，シュプリンガー・ジャパン，2006.

[73] Jozsa, R., Horodecki, M., Horodecki, P. and Horodecki, R., "Universal Quantum Information Compression," *Phys. Rev. Lett.*, **81**, 1714, 1998.

[74] Klappenecker, A. and Rötteler, M., "Beyond stabilizer codes II: Clifford

codes," *IEEE Trans. Inform. Theory*, **48**(8), 2396–2399, 2002.

[75] Klappenecker, A. and Sarvepalli, P. K., "Clifford code constructions of operator quantum error-correcting codes," *IEEE Trans. Inform. Theory*, **54**(12), 5760–5765, 2008.

[76] Klappenecker, A. and Sarvepalli, P. K., "Encoding Subsystem Codes," *International Journal on Advances in Security*, **2**(2–3), 142–155, 2009.

[77] Knill, E., "Group Representations, Error Bases and Quantum Codes," arXiv:quant-ph/9608049, 1996.

[78] Koashi, M. and Imoto, N., "Compressibility of Mixed-State Signals," *Phys. Rev. Lett.*, **87**, 017902, 2001.

[79] Von Korff, J. and Kempe, J., "Quantum Advantage in Transmitting a Permutation," *Phys. Rev. Lett.*, **93**(26), 260502, 2004.

[80] Kraus, K., *States, effects and operations*, Springer, 1983.

[81] Keyl, M. and Werner, R. F., "Estimating the spectrum of a density operator" *Phys. Rev. A*, **64**, 052311, 2001.

[82] Markham, D., Miyake, A. and Virmani, S., "Entanglement and local information access for graph states," *New J. Phys.*, **9**, 194, 2007.

[83] Marshall, A. W. and Olkin, I., *Inequalities: Theory of Majorization and Its Applications*, Academic Press, 1979.

[84] Matsumoto, R., "Conversion of a general quantum stabilizer code to an entanglement distillation protocol," *J. Phys. A: Math. and Gen.*, **36**(29), 8113–8127, 2003.

[85] Matsumoto, K. and Hayashi, M., "Universal distortion-free entanglement concentration," *Phys. Rev. A*, **75**, 062338, 2007.

[86] Matsumoto, K., Shimono, T. and Winter, A., "Remarks on additivity of the Holevo channel capacity and of the entanglement of formation," *Comm. Math. Phys.*, **246**(3), 427–442, 2004.

[87] Mayers, D., "Quantum key distribution and string oblivious transfer in noisy channels," *Advances in Cryptography Proceedings of Crypto '96*, 343–357, 1996.

[88] Mayers, D., "Unconditional security in quantum cryptography," *J. Assoc. Comp. Mach.*, **48**, 351–406, 2001.

[89] Miyadera, T., "Information-Disturbance Theorem for Mutually Unbiased Observables," *Phys. Rev. A*, **73**, 042317, 2006.

[90] Naĭmark, M. A., "On a representation of additive operator set functions," *Comptes Rendus (Doklady) de l'Academie des Sience de l'URSS*, **41**(9), 359, 1943.

[91] Nielsen, M. A. and Chuang, I. L., *Quantum Computation and Quantum*

Information, Cambridge University Press, Cambridge, 2000; 木村達也 訳, 『量子コンピュータと量子通信』(1)(2)(3), オーム社, 2004.

[92] Nielsen, M. A., "Conditions for a Class of Entanglement Transformations," *Phys. Rev. Lett.*, **83**, 436, 1999.

[93] Ohya, M. and Petz, D., *Quantum Entropy and Its Use*, Springer, New York, 1993.

[94] Owari, M., Plenio, M. B., Polzik, E. S., Serafini, A. and Wolf, M. M., "Squeezing the limit: quantum benchmarks for the teleportation and storage of squeezed states," *New J. Phys.*, **10**, 113014, 2008.

[95] Ozawa, M., "On the noncommutative theory of statistical decisions," *Research Reports on Information Sciences A*, **74**, 1980.

[96] Ozawa, M., "Quantum State Reduction and the Quantum Bayes Principle," in *Quantum Communication, Computing, and Measurement*, edited by Hirota, O., Holevo, A. S. and Caves, C. M., 233–241, Plenum, New York, 1997.

[97] Ozawa, M., "An Operational Approach to Quantum State Reduction," *Ann. Phys.*, **259**, 121–137, 1997.

[98] Ozawa, M., "Quantum State Reduction: An Operational Approach," *Fortschr. Phys.*, **46**, 615–625, 1998.

[99] Popescu, S., "Bell's inequalities versus teleportation: What is nonlocality?," *Phys. Rev. Lett.*, **72**, 797–799, 1994.

[100] Renner, R., "Security of quantum key distribution," PhD thesis, ETH Zurich, arXiv:quant-ph/0512258, 2005.

[101] Schumacher, B. and Westmoreland, M. D., "Sending classical information via noisy quantum channels," *Phys. Rev. A*, **56**, 131, 1997.

[102] Schumacher, B., "Sending entanglement through noisy quantum channels," *Phys. Rev. A*, **54**, 2614–2628, 1996.

[103] Schumacher, B. and Nielsen, M. A., "Quantum data processing and error correction," *Phys. Rev. A*, **54**, 2629, 1996.

[104] Shannon, C. E., "A Mathematical Theory of Communication," *Bell Sys. Tech. Jour.*, **27**, 379–423 and 623–656, 1948.

[105] Shimony, A., "Degree of entanglement," *Ann. N. Y. Acad. Sci.*, **755**, 675, 1995.

[106] Shor, P. and Preskill, J., "Simple proof of security of the BB84 quantumkey distribution protocol," *Phys. Rev. Lett.*, **85**, 441–444, 2000.

[107] Steane, A. M., "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. Lond. A*, **452**, 2551–2577, 1996.

[108] Stinespring, W. F., "Positive functions on C^* algebras," *Proc. Amer. Math.*

Soc., **6**, 211, 1955.

[109] Stinson, D. R., "Universal hash families and the leftover hash lemma, and applications to cryptography and computing," *J. Combin. Math. Combin. Comput.*, **42**, 3–31, 2002.

[110] Streltsov, A., Kampermann, H. and Bruß, D., "Linking a distance measure of entanglement to its convex roof," arXiv:1006.3077, 2010.

[111] Tsurumaru, T. and Hayashi, M., "Dual universality of hash functions and its applications to classical and quantum cryptography" *IEEE Trans. Inform. Theory*, **59**, 4700, 2013.

[112] Wang, X. B., Hiroshima, T., Tomita, A. and Hayashi, M., "Quantum Information with Gaussian States," *Physics Reports: a review section of physics letters*, **448**, Elsevier, 2007.

[113] Watanabe, S., Matsumoto, T. and Uyematsu, T., "Noise Tolerance of the BB84 Protocol with Random Privacy Amplification," *Int. J. Quant. Inform.*, **4**(6), 935–946, 2006.

[114] Wei, T.-C. and Goldbart, P. M., "Geometric measure of entanglement for bipartite and multipartite quantum states," *Phys. Rev. A*, **68**, 042307, 2003.

[115] Werner, R. F., "Optimal cloning of pure states," *Phys. Rev. A*, **58**, 1827, 1998.

[116] Wyner, A. D., "The wire-tap channel," *Bell Sys. Tech. Jour.*, **54**, 1355–1387, 1975.

[117] Vedral, V., Plenio, M. B., Rippin, M. A. and Knight, P. L., "Quantifying entanglement," *Phys. Rev. Lett.*, **78**, 2275, 1997.

[118] Vedral, V. and Plenio, M. B., "Entanglement Measures and Purification Procedures," *Phys. Rev. A*, **57**, 1619, 1998.

[119] Vidal, G. and Tarrach, R., "Robustness of entanglement" *Phys. Rev. A*, **59**, 141, 1999.

[120] Bouwmeester, D., Ekert, A. and Zeilinger, A. ed., *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Springer, 2000; 西野哲朗，井元信之 監訳，『量子情報の物理』，共立出版，2007.

[121] Mermin, N. D., *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007; 木村元 訳，『量子コンピュータ科学の基礎』，丸善出版，2009.

[122] Wilde, M. M., *Quantum Information Theory*, Cambridge University Press, 2013.

索　引

Memorandum

Memorandum

Memorandum

〈著者紹介〉

林　正人（はやし　まさひと）

1994年　京都大学理学部 卒業

1999年　京都大学大学院理学研究科博士後期課程（数学・数理解析専攻）修了
日本学術振興会特別研究員，理化学研究所脳科学総合研究センター研究員，科学技術振興機構 ERATO 今井量子計算機構プロジェクト技術参事，同 ERATO-SORST 量子情報システムアーキテクチャーグループリーダー，東北大学大学院情報科学研究科准教授を経て

現　在　名古屋大学大学院多元数理科学研究科 教授
博士（理学）

専　門　量子情報理論，量子暗号，情報理論

著　書　『量子情報理論入門』（サイエンス社，2004）
Asymptotic Theory Of Quantum Statistical Inference: Selected Papers
（編著，World Scientific Publishing，2005）
『量子情報科学入門』（共著，共立出版，2012）
『量子論のための表現論』（共立出版，2014）

量子情報への表現論的アプローチ

Group Representation Approach to Quantum Information

2014年 1 月25日　初版 1 刷発行

著　者　林　正人　© 2014

発行者　南條光章

発行所　**共立出版株式会社**

〒 112-8700
東京都文京区小日向 4-6-19
電話　03-3947-2511（代表）
振替口座　00110-2-57035
URL http://www.kyoritsu-pub.co.jp/

印　刷　啓文堂

製　本　中條製本

一般社団法人
自然科学書協会
会員

検印廃止

NDC 411.62, 007.1, 421.3

ISBN 978-4-320-11079-3

Printed in Japan